Product Guide

Revision B

# McAfee Advanced Threat Defense 3.2.0

## COPYRIGHT
Copyright © 2014 McAfee, Inc. Do not copy without permission.

## TRADEMARK ATTRIBUTIONS
McAfee, the McAfee logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundscore, Foundstone, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.

Product and feature names and descriptions are subject to change without notice. Please visit mcafee.com for the most current products and features.

## LICENSE INFORMATION

### License Agreement
NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

# Contents


**Preface** **7**

About this guide . . . . . 7

Conventions . . . . . 7

Find product documentation . . . . . 8

**1 Malware detection and McAfee® Advanced Threat Defense** **9**

The malware threat scenario . . . . . 9

The McAfee Advanced Threat Defense solution . . . . . 10

McAfee Advanced Threat Defense deployment options . . . . . 12

McAfee Advanced Threat Defense advantages . . . . . 14

**2 Setting up the McAfee Advanced Threat Defense Appliance** **17**

About McAfee Advanced Threat Defense Appliance . . . . . 17

Functions of a McAfee Advanced Threat Defense Appliance . . . . . 17

Before you install the McAfee Advanced Threat Defense Appliance . . . . . 18

Warnings and cautions . . . . . 19

Usage restrictions . . . . . 19

Unpack the shipment . . . . . 20

Check your shipment . . . . . 20

Hardware specifications and environmental requests . . . . . 23

Port numbers . . . . . 25

Setting up McAfee Advanced Threat Defense . . . . . 25

Install or remove rack handles . . . . . 26

Install or remove the Appliance from the rack . . . . . 26

Turn on the McAfee Advanced Threat Defense Appliance . . . . . 28

Handling the front bezel . . . . . 28

Connect the network cable . . . . . 29

Configure network information for McAfee Advanced Threat Defense Appliance . . . . . 29

**3 Accessing McAfee Advanced Threat Defense web application** **33**

McAfee Advanced Threat Defense client requirements . . . . . 33

Access the McAfee Advanced Threat Defense web application . . . . . 34

**4 Managing Advanced Threat Defense** **35**

Managing McAfee Advanced Threat Defense users . . . . . 35

Viewing user profiles . . . . . 36

Add users . . . . . 37

Edit Users . . . . . 40

Delete Users . . . . . 40

Monitoring the McAfee Advanced Threat Defense performance . . . . . 40

Upgrade McAfee Advanced Threat Defense and Android VM . . . . . 40

Upgrade McAfee Advanced Threat Defense software from 3.0.2.xx to 3.0.4.xx . . . . . 41

Upgrade McAfee Advanced Threat Defense software from 3.0.2.36 to 3.2.0.xx . . . . . 44

Upgrade McAfee Advanced Threat Defense software from 3.0.4.xx to 3.2.0.xx . . . . . 47

Upgrade the Android analyzer VM . . . . . 49

Troubleshooting . . . 52
Export McAfee Advanced Threat Defense logs . . . 52
Recreate the analyzer VMs . . . 53
Delete the analysis results . . . 54
Backup and restore McAfee Advanced Threat Defense database . . . 54
Schedule a database backup . . . 55
Restore a database backup . . . 58

**5 Creating analyzer VM 61**
Create a VMDK file for Windows XP . . . 62
Create a VMDK file for Windows 2003 Server . . . 90
Create a VMDK file for Windows 7 . . . 119
Create a VMDK file for Windows 2008 Server . . . 145
Create a VMDK file for Windows 8 . . . 171
Import a VMDK file into McAfee Advanced Threat Defense . . . 208
Convert the VMDK file to an image file . . . 209
Managing VM profiles . . . 212
View VM profiles . . . 213
Create VM profiles . . . 214
Edit VM profiles . . . 219
Delete VM profiles . . . 220
View the VM creation log . . . 220

**6 Configuring McAfee Advanced Threat Defense for malware analysis 221**
Terminologies . . . 221
High-level steps for configuring malware analysis . . . 225
How McAfee Advanced Threat Defense analyzes malware? . . . 225
Internet access to sample files . . . 226
Managing analyzer profiles . . . 229
View analyzer profiles . . . 230
Create analyzer profiles . . . 231
Edit analyzer profiles . . . 233
Delete analyzer profiles . . . 233
Integration with McAfee ePO . . . 234
Configure McAfee ePO integration . . . 235
Specify proxy server for internet connectivity . . . 235
Configure the proxy DNS settings . . . 236
Configure date and time settings . . . 237
Define custom YARA rules for identifying malware . . . 240
Create the custom YARA rules file . . . 242
Import the custom YARA rules file . . . 245
Enable or disable custom YARA rules . . . 245
Modify custom YARA rules . . . 246

**7 Analyzing malware 247**
Analyze files . . . 247
Upload files for analysis using McAfee Advanced Threat Defense web application . . . 248
Upload files for analysis using SFTP . . . 254
Analyze URLs . . . 254
How Advanced Threat Defense analyzes URLs? . . . 255
Upload URLs for analysis using Advanced Threat Defense web application . . . 255
Monitor the status of malware analysis . . . 257
View the analysis results . . . 259
View the Analysis Summary report . . . 261
Dropped files report . . . 267
Disassembly Results . . . 267

Logic Path Graph . . . 268
User API Log . . . 273
Download the complete results .zip file . . . 273
Working with the McAfee Advanced Threat Defense Dashboard . . . 274
Malware analysis monitors . . . 275
VM Creation Status monitor . . . 278
McAfee Advanced Threat Defense performance monitors . . . 278

**8 Clustering McAfee Advanced Threat Defense Appliances 281**
Understanding McAfee Advanced Threat Defense cluster . . . 281
Pre-requisites and considerations . . . 282
Network connections for an Advanced Threat Defense cluster . . . 283
How the Advanced Threat Defense cluster works? . . . 284
Process flow for Network Security Platform . . . 287
Process flow for McAfee Web Gateway . . . 288
Configuring an Advanced Threat Defense cluster - high-level steps . . . 289
Create the McAfee Advanced Threat Defense cluster . . . 290
Monitor the status of an Advanced Threat Defense cluster . . . 293
Submitting samples to an Advanced Threat Defense cluster . . . 296
Monitor analysis status for an Advanced Threat Defense cluster . . . 296
Monitor analysis results for an Advanced Threat Defense cluster . . . 297
Modifying configurations for a McAfee Advanced Threat Defense cluster . . . 298

**9 CLI commands for McAfee Advanced Threat Defense 299**
Issue of CLI commands . . . 299
How to issue a command through the console . . . 299
Issuing a command through SSH . . . 299
Logging on to the McAfee Advanced Threat Defense Appliance using an SSH client . . . 300
Auto-complete . . . 300
CLI syntax . . . 300
Mandatory commands . . . 300
Log on to the CLI . . . 301
Meaning of "?" . . . 301
Managing the disks of McAfee Advanced Threat Defense Appliance . . . 301
List of CLI commands . . . 302
amas . . . 302
atdcounter . . . 302
backup reports . . . 302
backup reports date . . . 303
Blacklist . . . 303
clearstats . . . 304
createDefaultVms . . . 304
db_repair . . . 304
deleteblacklist . . . 304
deletesamplereport . . . 304
diskcleanup . . . 305
Exit . . . 305
factorydefaults . . . 305
ftptest USER_NAME . . . 305
gti-restart . . . 306
help . . . 306
heuristic_analysis . . . 306
lbstats . . . 308
list . . . 308
lowseveritystatus . . . 308
nslookup . . . 309

passwd . . . 309
ping . . . 309
quit . . . 310
reboot . . . 310
resetuiadminpasswd . . . 310
resetusertimeout . . . 310
route add/delete network . . . 310
samplefilter . . . 311
set appliance ip . . . 311
set appliance gateway . . . 312
set appliance name . . . 312
set intfport . . . 312
set intfport auto . . . 312
set intfport ip . . . 313
set intfport speed duplex . . . 313
set malware-intfport . . . 313
set mgmtport auto . . . 313
set mgmtport speed and duplex . . . 314
set fips . . . 314
set ftp . . . 314
set heuristic_analysis . . . 314
set ui-timeout . . . 314
set whitelist . . . 315
show . . . 315
show epo-stats nsp . . . 315
show fips . . . 315
show ftp . . . 316
show history . . . 316
show heuristic_analysis . . . 316
show intfport . . . 316
show nsp scandetails . . . 317
show route . . . 317
show ui-timeout . . . 318
shutdown . . . 318
status . . . 318
update_avdat . . . 319
Vmlist . . . 319
watchdog . . . 319
set malware-intfport mgmt . . . 319
whitelist . . . 319

**Index** **321**

# Preface

This guide provides the information you need to work with your McAfee product.

**Contents**


- *About this guide*
- *Find product documentation*


## About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

### Conventions

This guide uses these typographical conventions and icons.

| | |
|---|---|
| *Book title*, *term*, *emphasis* | Title of a book, chapter, or topic; a new term; emphasis. |
| **Bold** | Text that is strongly emphasized. |
| `User input, code, message` | Commands and other text that the user types; a code sample; a displayed message. |
| **Interface text** | Words from the product interface like options, menus, buttons, and dialog boxes. |
| Hypertext blue | A link to a topic or to an external website. |
| | **Note:** Additional information, like an alternate method of accessing an option. |
| | **Tip:** Suggestions and recommendations. |
| | **Important/Caution:** Valuable advice to protect your computer system, software installation, network, business, or data. |
| | **Warning:** Critical advice to prevent bodily harm when using a hardware product. |

# Find product documentation

After a product is released, information about the product is entered into the McAfee online Knowledge Center.

## Task

1 Go to the McAfee ServicePortal at http://support.mcafee.com and click **Knowledge Center**.

2 Enter a product name, select a version, then click **Search** to display a list of documents.

# 1 Malware detection and McAfee® Advanced Threat Defense

Over the years, malware has evolved into a sophisticated tool for malicious activities such as stealing valuable information, accessing your computer resources without your knowledge, and for disrupting business operations. At the same time, technological advancement provides limitless options to deliver malicious files to unsuspecting users. Hundreds of thousands of new malware variants every day make the job of malware detection even more complex. Traditional anti-malware techniques are no longer sufficient to protect your network.

McAfee's response to this challenge is the McAfee Advanced Threat Defense solution. This is an on-premise Appliance that facilitates detection and prevention of malware. McAfee Advanced Threat Defense provides protection from known, near-zero day, and zero-day malware without compromising on the quality of service to your network users.

McAfee Advanced Threat Defense has the added advantage of being an integrated solution. In addition to its own multi-level threat detection capabilities, its ability to seamlessly integrate with other McAfee security products, protects your network against malware and other Advanced Persistent Threats (APTs).

**Contents**


- *The malware threat scenario*
- *The McAfee Advanced Threat Defense solution*


## The malware threat scenario

Any software capable of being involved in hostile activities with respect to a computer, application, or network can be termed as malware. McAfee Advanced Threat Defense is designed for detecting file-based malware.

Earlier, users received malware as attachments in their emails. With the upsurge in Internet applications, users only need to click a link to download files. Today, there are many other options to post such files — blogs, social networking sites, web sites, chat messages, web mails, message boards, and so on. The key challenges in tackling this issue are to detect malware in the shortest possible time and also contain it from spreading to other computers.

There are four major aspects to an anti-malware strategy:

- Detection of file downloads: When a user attempts to download a file from an external resource, your security product must be able to detect it.
- Analysis of the file for malware: You must be able to verify if the file contains any known malware.

- Block future downloads of the same file: Subsequently, if the file is found to be malicious, your anti-malware protection must prevent future downloads of the same file or its variants.
- Identify and remediate affected hosts: Your security system must be able to identify the host which executed the malware, and also detect the hosts to which it has spread. Then, it must provide an option to quarantine the affected hosts until they are clean again.

# The McAfee Advanced Threat Defense solution

A security solution that relies on a single method or process might not be adequate to provide complete and reliable protection from malware attacks. You might need a multi-layered solution that involves various techniques and products. The solution can include pattern matching, global reputation, program emulation, static analysis, and dynamic analysis. All these layers must be seamlessly integrated and provide you with a single point of control for easy configuration and management. For example, pattern matching might not detect zero-day attacks. Similarly, static analysis takes less time than dynamic analysis. However, malware can avoid static analysis by code obfuscation. Malware can escape dynamic analysis too by delaying execution or take an alternate execution path if the malware detects that it is being run in a sandbox environment. This is why a reliable protection from malware requires a multi-level approach.

There are other industry-leading McAfee anti-malware products for the web, network, and endpoints. However, McAfee recognizes that a robust anti-malware solution requires a multi-layered approach, the result of which is McAfee Advanced Threat Defense.

The McAfee Advanced Threat Defense solution primarily consists of the McAfee Advanced Threat Defense Appliance and the pre-installed software. The McAfee Advanced Threat Defense Appliance is available in two models. The standard model is the ATD-3000. The high-end model is the ATD-6000.

McAfee Advanced Threat Defense integrates its native capabilities with other McAfee products to provide you a multilayered defense mechanism against malware:

- Its preliminary detection mechanism consists of a local blacklist to quickly detect known malware.
- It integrates with McAfee® Global Threat Intelligence™ (McAfee GTI) for cloud-lookups to detect malware that has already been identified by organizations throughout the globe.
- It has the McAfee Gateway Anti-Malware Engine embedded within it for emulation capability.

- It has the McAfee Anti-Malware Engine embedded within it for signature-based detection.
- It dynamically analyzes the file by executing it in a virtual sandbox environment. Based on how the file behaves, McAfee Advanced Threat Defense determines its malicious nature.

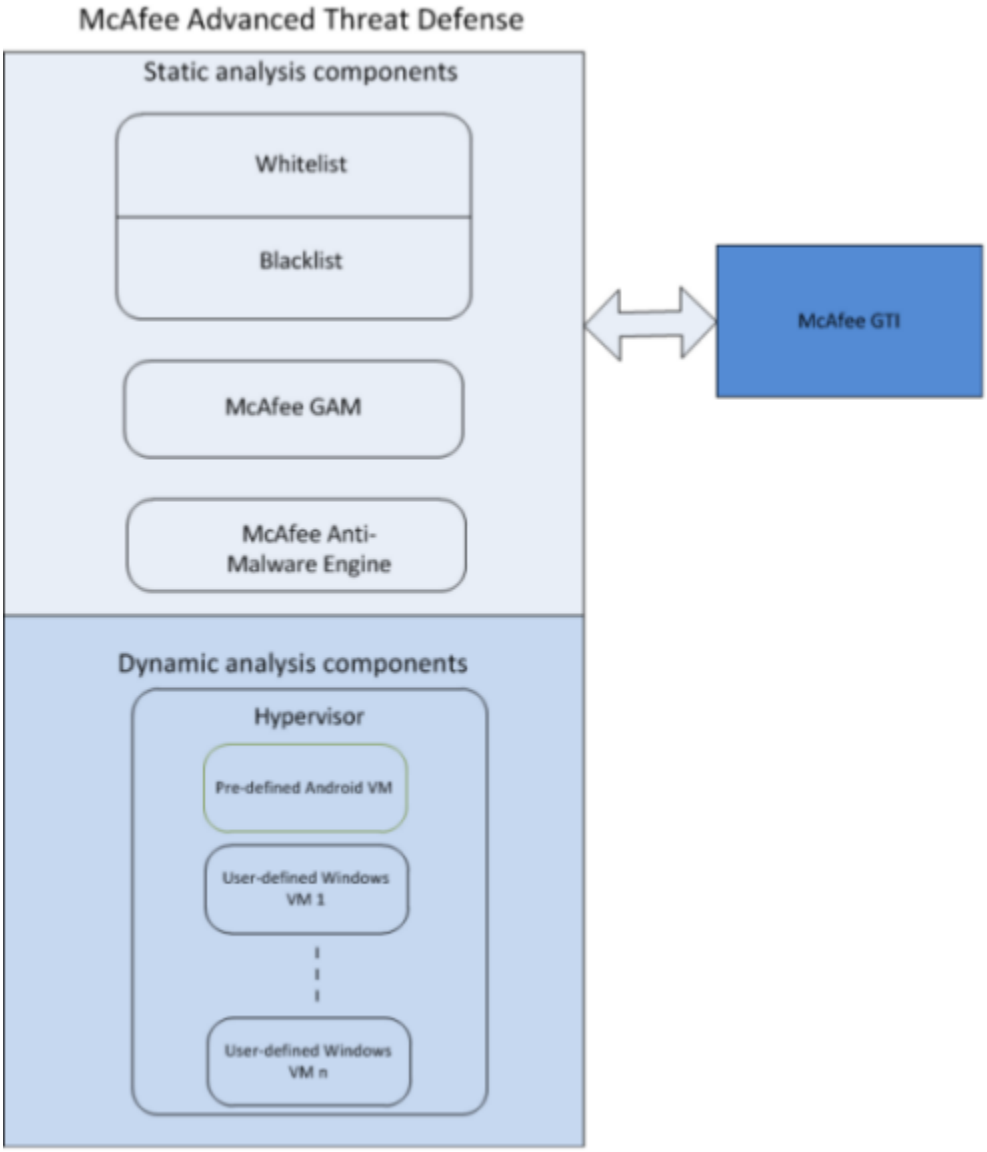



**Figure 1-1 Components for malware analysis**

## McAfee Advanced Threat Defense deployment options

You can deploy McAfee Advanced Threat Defense in the following ways:

- Standalone deployment — This is a simple way of deploying McAfee Advanced Threat Defense. In this case, it is not integrated with other externally installed McAfee products. When deployed as a standalone Appliance, you can manually submit the suspicious files using the McAfee Advanced Threat Defense web application. Alternatively, you can submit the samples using an FTP client. This deployment option is used, for example, during the testing and evaluation phase, to fine-tune configuration, and to analyze suspicious files in an isolated network segment. Also, research engineers might use the standalone deployment option for detailed analysis of malware.

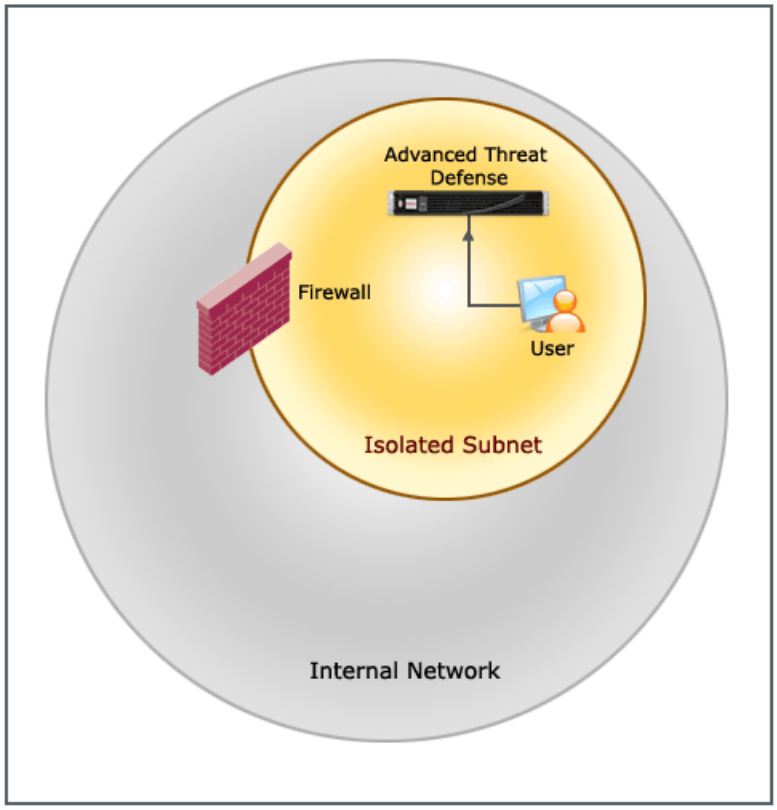



**Figure 1-2 A standalone deployment scenario**

- Integration with Network Security Platform — This deployment involves integrating McAfee Advanced Threat Defense with Network Security Platform Sensor and Manager.

  Based on how you have configured the corresponding Advanced Malware policy, an inline Sensor detects a file download and sends a copy of the file to McAfee Advanced Threat Defense for analysis. If McAfee Advanced Threat Defense detects a malware within a few seconds, the Sensor can block the download. The Manager displays the results of the analysis from McAfee Advanced Threat Defense.

  If McAfee Advanced Threat Defense requires more time for analysis, the Sensor allows the file to be downloaded. If McAfee Advanced Threat Defense detects a malware after the file has been downloaded, it informs Network Security Platform, and you can use the Sensor to quarantine the host until it is cleaned and remediated. You can configure the Manager to update all the Sensors about this malicious file. Therefore, if that file is downloaded again anywhere in your network, your Sensors might be able to block it.

  For information on how to integrate Network Security Platform and McAfee Advanced Threat Defense, refer to the latest *Network Security Platform Integration Guide.*

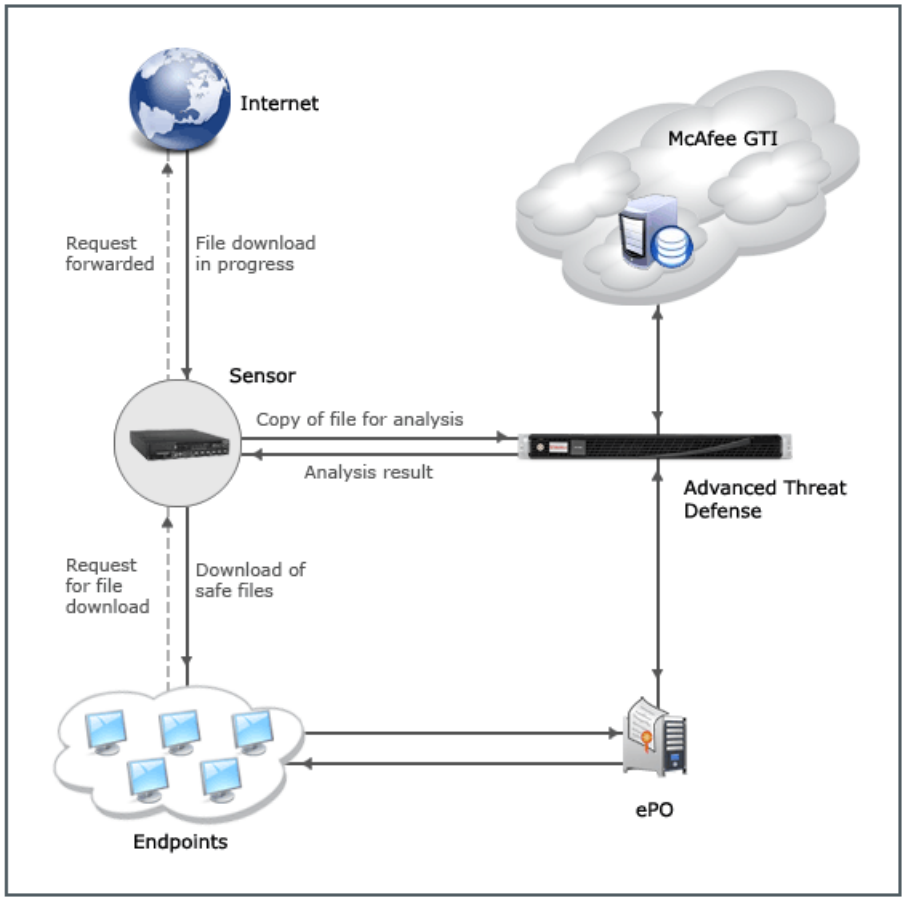



**Figure 1-3 Integration with Network Security Platform and McAfee ePO**

- Integration with McAfee® Web Gateway — You can configure McAfee Advanced Threat Defense as an additional engine for anti-malware protection. When your network user downloads a file, the native McAfee Gateway Anti-malware Engine on McAfee® Web Gateway scans the file and determines a malware score. Based on this score and the file type, McAfee® Web Gateway sends a copy of the file to McAfee Advanced Threat Defense for deeper inspection and dynamic analysis. A progress page informs your users that the requested file is being analyzed for malware. Based on the malware severity level reported by McAfee Advanced Threat Defense, McAfee® Web Gateway determines if the file is allowed or blocked. If it is blocked, the reasons are displayed for your users. You can view the details of the malware that was detected in the log file.

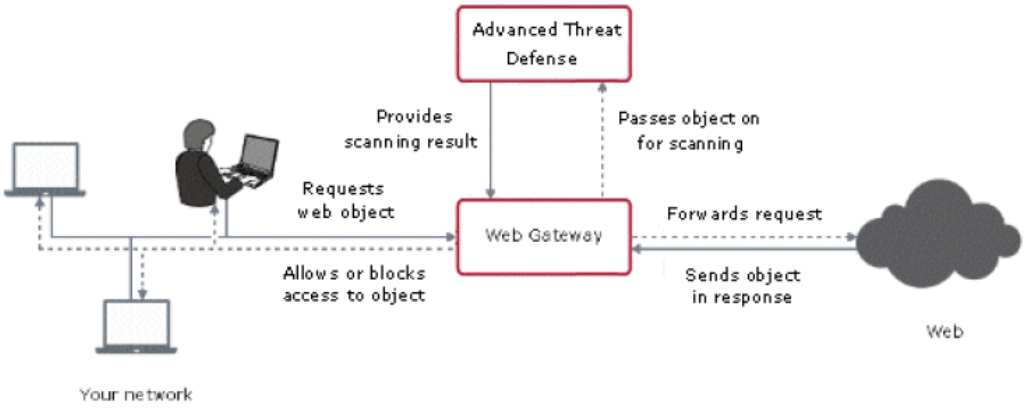



**Figure 1-4 Integration with McAfee® Web Gateway**

This design ensures that only those files that require an in-depth analysis are sent to McAfee Advanced Threat Defense. This balances your users' experience in terms of download speed and security. For information on how to integrate McAfee Advanced Threat Defense and McAfee® Web Gateway, see the *McAfee® Web Gateway Product Guide,* version 7.4.

- Integration with McAfee® ePolicy Orchestrator (McAfee ePO) — This integration enables McAfee Advanced Threat Defense to retrieve information regarding the target host. Knowing the operating system on the target host, enables it to select a similar virtual environment for dynamic analysis.

How the deployment options address the 4 major aspects of anti-malware process cycle:

- Detection of file download: As soon as a user accesses a file, the inline Network Security Platform Sensor or McAfee® Web Gateway detects this and sends a copy of the file to McAfee Advanced Threat Defense for analysis.
- Analysis of the file for malware: Even before the user fully downloads the file, McAfee Advanced Threat Defense can detect a known malware using sources that are local to it or on the cloud.
- Block future downloads of the same file: Every time McAfee Advanced Threat Defense detects a medium, high, or very high severity malware, it updates its local black list.
- Identify and remediate affected hosts: Integration with Network Security Platform enables you to quarantine the host until it is cleaned up and remediated.

## McAfee Advanced Threat Defense advantages

Here are some of the advantages that McAfee Advanced Threat Defense provides:

- It is an on-premises solution that has access to cloud-based GTI. In addition, you can integrate it with other McAfee's security products.
- McAfee Advanced Threat Defense does not sniff or tap into your network traffic. It analyzes the files submitted to it for malware. This means that you can place the McAfee Advanced Threat Defense Appliance anywhere in your network as long as it is reachable to all the integrated McAfee products. It is also possible for one McAfee Advanced Threat Defense Appliance to cater to all such integrated products (assuming the number of files submitted is within the supported level). This design can make it a cost-effective and scalable anti-malware solution.
- McAfee Advanced Threat Defense is not an inline device. It can receive files from IPS Sensors for malware analysis. So, it is possible to deploy McAfee Advanced Threat Defense in such a way that you obtain the advantages of an inline anti-malware solution but without the associated drawbacks.
- Android is currently one of the top targets for malware developers. With this integration, the Android-based handheld devices on your network are also protected. You can dynamically analyze the files downloaded by your Android devices such as smartphones and tablets.
- Files are concurrently analyzed by various engines. So, it is possible for known malware to be blocked in almost real time.
- When McAfee Advanced Threat Defense dynamically analyzes a file, it selects the analyzer virtual machine that uses the same operating system and other applications as that of the target host. This is achieved through its integration with McAfee ePO or through passive device profiling feature of Network Security Platform. This enables you to identify the exact impact on a targeted host, so that you can take the required remedial measures. This also means that McAfee Advanced Threat Defense executes the file only the required virtual machine, reserving its resources for other files.
- Consider a host downloaded a zero-day malware, but a Sensor that detected this file downloaded submitted it to McAfee Advanced Threat Defense. After a dynamic analysis, McAfee Advanced Threat Defense determines the file to be malicious. Based on how you have configured the Advanced Malware policy, it is possible for the Manager to add this malware to the blacklist of all the Sensors in your organization's network. This file also might be on the blacklist of McAfee Advanced Threat Defense. Thus, the chances of the same file re-entering your network is reduced.
- Even the first time when a zero-day malware is downloaded, you can contain it by quarantining the affected hosts until they are cleaned and remediated.
- Packing can change the composition of the code or enable a malware to evade reverse engineering. So, proper unpacking is very critical to get the actual malware code for analysis. McAfee Advanced Threat Defense is capable of unpacking the code such that the original code is secured for static analysis.

# 2 Setting up the McAfee Advanced Threat Defense Appliance

Review this chapter for information regarding the McAfee Advanced Threat Defense Appliance and how to set it up.

**Contents**


- *About McAfee Advanced Threat Defense Appliance*
- *Functions of a McAfee Advanced Threat Defense Appliance*
- *Before you install the McAfee Advanced Threat Defense Appliance*
- *Hardware specifications and environmental requests*
- *Setting up McAfee Advanced Threat Defense*


## About McAfee Advanced Threat Defense Appliance

Depending on the model, the McAfee Advanced Threat Defense Appliance is a 1-U or 2-U rack dense chassis with Intel® Xeon® E5-2600 product family processor. The McAfee Advanced Threat Defense Appliance runs on a pre-installed, hardened Linux kernel 3.6.0 and comes preloaded with the McAfee Advanced Threat Defense software.

The McAfee Advanced Threat Defense Appliance is available in the following models:

- ATD-3000: This standard model is a 1U chassis.
- ATD-6000: This high-end model is a 2U chassis.

## Functions of a McAfee Advanced Threat Defense Appliance

The McAfee Advanced Threat Defense Appliances are purpose-built, scalable, and flexible high-performance servers designed to analyze suspicious files for malware.

The following are the primary functions of the McAfee Advanced Threat Defense Appliance:

- Host the McAfee Advanced Threat Defense software that analyzes files for malware.
- Host the McAfee Advanced Threat Defense web application.
- Host the virtual machines used for dynamic analysis of suspicious files.

For the performance values related to ATD-3000 and ATD-6000, contact McAfee support.

# Before you install the McAfee Advanced Threat Defense Appliance

This section describes the tasks that you must complete before you begin to install a McAfee Advanced Threat Defense.

- Read all the provided documentation before installation.
- Make sure that you have selected a suitable location for installing the McAfee Advanced Threat Defense Appliance.
- Check that you have all the necessary equipment and components outlined in this document.
- Familiarize yourself with the McAfee Advanced Threat Defense Appliance network access card (NIC) ports and connectors as described in this document.
- Make sure you have the following information available when you configure the McAfee Advanced Threat Defense Appliance:
  - IPv4 address that you want to assign to the Appliance.
  - Network mask.
  - Default gateway address.

## Warnings and cautions

Read and follow these safety warnings when you install the McAfee Advanced Threat Defense Appliance. Failure to observe these safety warnings could result in serious physical injury.

- McAfee Advanced Threat Defense Appliance power on/off — the push-button on/off power switch on the front panel of the McAfee Advanced Threat Defense Appliance does not turn off the AC power. To remove AC power from the McAfee Advanced Threat Defense Appliance, you must unplug the AC power cord from either the power supply or wall outlet for both the power supplies.
- The power supplies in your system might produce high voltages and energy hazards, which can cause bodily harm. Only trained service technicians are authorized to remove the covers and access any of the components inside the system.
- Hazardous conditions — devices and cables: Hazardous electrical conditions might be present on power, telephone, and communication cables. Turn off the McAfee Advanced Threat Defense Appliance and disconnect telecommunications systems, networks, modems, and both the power cords attached to the McAfee Advanced Threat Defense Appliance before opening it. Otherwise, personal injury or equipment damage can result.
- Avoid injury — lifting the McAfee Advanced Threat Defense Appliance and attaching it to the rack is a two-person job.
- This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.
- Do not remove the outer shell of the McAfee Advanced Threat Defense Appliance. Doing so invalidates your warranty.
- Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place. Blank faceplates and cover panels prevent exposure to hazardous voltages and currents inside the chassis, contain electromagnetic interference (EMI) that might disrupt other equipment and direct the flow of cooling air through the chassis.
- To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.

## Usage restrictions

The following restrictions apply to the use and operation of McAfee Advanced Threat Defense Appliance:

- You should not remove the outer shell of the McAfee Advanced Threat Defense Appliance. Doing so invalidates your warranty.
- The McAfee Advanced Threat Defense Appliance is not a general purpose server.
- McAfee prohibits the use of McAfee Advanced Threat Defense Appliance for anything other than operating the McAfee Advanced Threat Defense solution.
- McAfee prohibits the modification or installation of any hardware or software on the McAfee Advanced Threat Defense Appliance that is not part of the normal operation of McAfee Advanced Threat Defense.

## Unpack the shipment

1. Open the crate.
2. Remove the first accessory box.
3. Verify you have received all parts as listed in Check your shipment on page 20.
4. Remove the McAfee Advanced Threat Defense Appliance.
5. Place the McAfee Advanced Threat Defense Appliance as close to the installation site as possible.
6. Position the box with the text upright.
7. Open the top flaps of the box.
8. Remove the accessory box within the McAfee Advanced Threat Defense Appliance box.
9. Remove the slide rail kit.
10. Pull out the packing material surrounding the McAfee Advanced Threat Defense Appliance.
11. Remove the McAfee Advanced Threat Defense Appliance from the anti-static bag.
12. Save the box and packing materials for later use in case you need to move or ship the McAfee Advanced Threat Defense Appliance.

## Check your shipment

The following accessories are shipped in the McAfee Advanced Threat Defense Appliance crate:

- McAfee Advanced Threat Defense Appliance
- Accessories itemized on the *Content Sheet*
- Set of tool-less slide rails
- Front bezel with key

## McAfee Advanced Threat Defense Appliance front and back panels

**Figure 2-1 Front view of ATD-3000 with bezel**

**Figure 2-2 Side view of ATD-3000 without bezel**

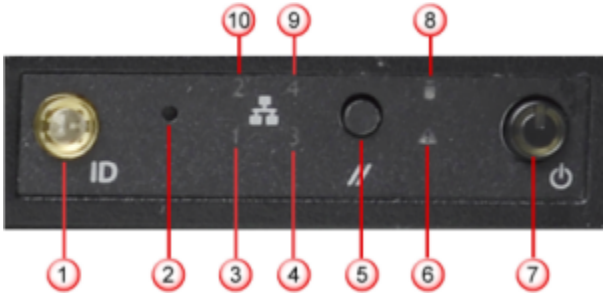



**Figure 2-3 ATD-3000 and ATD-6000 front panel**

| Label | Description |
|---|---|
| 1 | System ID button with integrated indicator light |
| 2 | NMI button (recessed, tool required for use) |
| 3 | NIC 1 activity indicator light |
| 4 | • ATD-3000: NIC 3 activity indicator light<br>• ATD-6000: Not used |
| 5 | System cold reset button |
| 6 | System status indicator light |
| 7 | Power button with integrated indicator light |
| 8 | Hard drive activity indicator light |
| 9 | • ATD-3000: NIC 4 activity indicator light<br>• ATD-6000: Not used |
| 10 | NIC 2 activity indicator light |

An optional, lockable bezel is included with the McAfee Advanced Threat Defense Appliance, which you can install to cover the front panel.

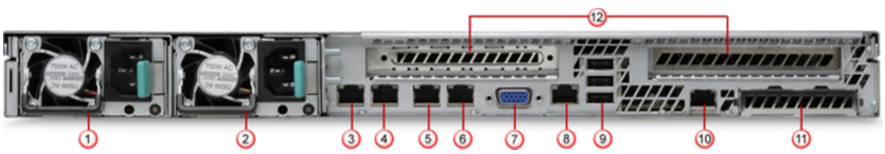



**Figure 2-4 ATD-3000 Appliance back panel**

| Label | Description |
|---|---|
| 1 | Power supply module 1 |
| 2 | Power supply module 2 |
| 3 | Management port (NIC 1). This is the eth-0 interface. The `set appliance` and `set mgmtport` commands apply to this interface. For example, when you use the `set appliance ip` command, the corresponding IP address is assigned to this interface. |
| 4 | NIC 2. This is the eth-1 interface. This interface is disabled by default.<br>• To enable or disable this interface, use the `set intfport` command. For example, `set intfport 1 enable`<br>• To assign the IP details to this interface use `set intfport <eth 1, 2, or 3> ip <IPv4 address> <subnet mask>`<br>For example, `set intfport 1 ip 10.10.10.10 255.255.255.0`<br>• You cannot assign the default gateway to this port. However, you can configure a route on this interface to route the traffic to the desired gateway. To configure a route, use `route add network <IPv4 subnet> netmask <netmask> gateway <IPv4 address> intfport 1`<br>For example, `route add network 10.10.10.0 netmask 255.255.255.0 gateway 10.10.10.1 intfport 1`. This command routes all traffic from the 10.10.10.0 command to 10.10.10.1 through NIC 2 (eth-1). |
| 5 | NIC 3. This is the eth-2 interface. The note described for NIC 2 applies to this interface as well. |
| 6 | NIC 4. This is the eth-3 interface. The note described for NIC 2 applies to this interface as well. |
| 7 | Video connector |
| 8 | RJ45 serial-A port |
| 9 | USB ports |
| 10 | RMM4 NIC port |
| 11 | I/O module ports/connectors (not used) |
| 12 | Add-in adapter slots from riser card 1 and riser card 2 |

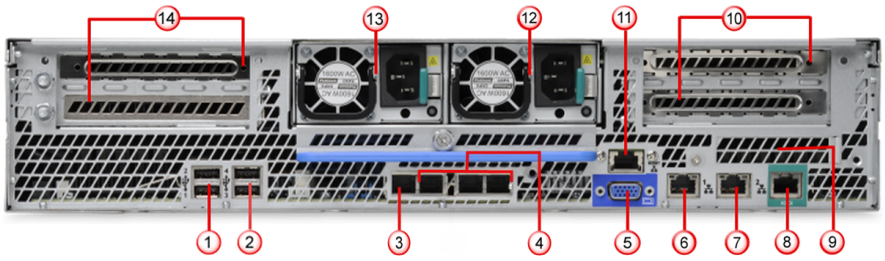



**Figure 2-5 ATD-6000 Appliance back panel**

| Label | Description |
|---|---|
| 1 | USB ports |
| 2 | USB ports |
| 3 | Management port. This is the eth-0 interface. The `set appliance` and `set mgmtport` commands apply to this interface. For example, when you use the `set appliance ip` command, the corresponding IP address is assigned to this interface. |

| Label | Description |
|---|---|
| 4 | Additional I/O module ports/connectors. These are the eth-1, eth-2, and eth-3 interfaces respectively. These interfaces are disabled by default.<br>• To enable or disable an interface, use the `set intfport` command. For example, `set intfport 1 enable` to enable eth-1.<br>• To assign the IP details to an interface use `set intfport <eth 1, 2, or 3> ip <IPv4 address> <subnet mask>`<br>For example, `set intfport 1 ip 10.10.10.10 255.255.255.0`<br>• You cannot assign the default gateway to this port. However, you can configure a route on this interface to route the traffic to the desired gateway. To configure a route, use `route add network <IPv4 subnet> netmask <netmask> gateway <IPv4 address> intfport 1`<br>For example, `route add network 10.10.10.0 netmask 255.255.255.0 gateway 10.10.10.1 intfport 1`. This command routes all traffic from the 10.10.10.0 command to 10.10.10.1 through eth-1. |
| 5 | Video connector |
| 6 | NIC 1 (currently not used) |
| 7 | NIC 2 (currently not used) |
| 8 | RJ45 serial-A port |
| 9 | I/O module ports/connectors (not used) |
| 10 | Add-in adapter slots from riser card |
| 11 | RMM4 NIC port |
| 12 | Power supply module 2 |
| 13 | Power supply module 1 |
| 14 | Add-in adapter slots from riser card |

# Hardware specifications and environmental requests

| Specifics | ATD-3000 | ATD-6000 |
|---|---|---|
| **Dimensions** | • 734.66 L x 438 W x 43.2 H in millimeters<br>• 29 L x 17.25 W x 1.70 H in inches | • 712 L x 438 W x 87.3 H in millimeters<br>• 28 L x 17.24 W x 3.43 H in inches |
| **Form Factor** | 1U rack mountable; fits 19-inch rack | 2U rack mountable; fits 19-inch rack |
| **Weight** | 15 Kg (33 lbs) | 22.7 Kg (50 lbs.) |
| **Storage** | • Disk space HDD: 2 x 4TB<br>• SSD: 2 x 400 GB | • Disk space HDD: 4 x 4TB<br>• SSD: 2 x 800 GB |
| **Maximum Power Consumption** | 2x 750W | 2x 1600W |
| **Redundant Power Supply** | AC redundant, hot swappable | AC redundant, hot swappable |
| **AC voltage** | 100 - 240 V at 50 - 60 Hz. 5.8 Amps | 100 - 240 V. 50 - 60 Hz. 8.5 Amps |

| Specifics | ATD-3000 | ATD-6000 |
|---|---|---|
| **Operating Temperature** | +10°C to +35° C (+50°F to + 95°F) with the maximum rate of change not to exceed 10°C per hour | +10º C to +35º C (+50ºF to +95ºF) with the maximum rate of change not to exceed 10°C per hour |
| **Non-operating temperature** | -40°C to +70°C (-40°F to +158°F) | -40°C to +70°C (-40°F to +158°F) |
| **Relative humidity (non-condensing)** | • Operational: 10% to 90%<br>• Non-operational: 90% at 35°C | • Operational: 10% to 90%<br>• Non-operational: 50% to 90% with a maximum wet bulb of 28°C (at temperatures from 25°C to 35°C) |
| **Altitude** | Support operation up to 3050 meters (10,000 feet) | Support operation up to 3050 meters (10,000 feet) |
| **Safety Certification** | UL 1950, CSA-C22.2 No. 950, EN-60950, IEC 950, EN 60825, 21CFR1040 CB license and report covering all national country deviations | UL 1950, CSA-C22.2 No. 950, EN-60950, IEC 950, EN 60825, 21CFR1040 CB license and report covering all national country deviations |
| **EMI Certification** | FCC Part 15, Class A (CFR 47) (USA) ICES-003 Class A (Canada), EN55022 Class A (Europe), CISPR22 Class A (Int'l) | FCC Part 15, Class A (CFR 47) (USA) ICES-003 Class A (Canada), EN55022 Class A (Europe), CISPR22 Class A (Int'l) |
| **Acoustic noise** | Sound power: 7.0 BA in operating conditions at typical office ambient temperature (23 +/- 2 degrees C). | Sound power: 7.0 BA in operating conditions at typical office ambient temperature (23 +/- 2 degrees °C). |
| **Shock, operating** | Half sine, 2 g peak, 11 milliseconds | Half sine, 2 g peak, 11 milliseconds |
| **Shock, unpackaged** | Trapezoidal, 25 g, velocity change 136 inches/second (≧40 lbs to < 80 lbs) | Trapezoidal, 25 g, velocity change is based on packaged weight |
| **Shock, packaged** | Non-palletized free fall in height 24 inches (≧40 lbs to < 80 lbs) | • Product Weight: ≥ 40 to < 80<br>• Non-palletized Free Fall Height = 18 inches<br>• Palletized (single product) Free Fall Height = NA |
| **Vibration** | Unpackaged: 5 Hz to 500 Hz, 2.20 g RMS random | Unpackaged: 5 Hz to 500 Hz, 2.20 g RMS random<br>Packaged: 5 Hz to 500 Hz, 1.09 g RMS random |
| **ESD** | +/-12 KV except I/O port +/- 8 KV per Intel® Environmental test specification | Air Discharged: 12.0 kV<br>Contact Discharge: 8.0 kV |
| **System cooling requirement in BTU/Hr** | • 460 Watt Max – 1570 BTU/hour<br>• 750 Watt Max – 2560 BTU/hour | • 460 Watt Max – 1570 BTU/hour<br>• 750 Watt Max – 2560 BTU/hour |
| **Memory** | 192 GB | 256 GB |

## Port numbers

**Table 2-1 Port numbers**

| Client | Server | Default port | Configurable | Description |
|---|---|---|---|---|
| Any (desktop) | McAfee Advanced Threat Defense | TCP 443 (HTTPS) | No | Access McAfee Advanced Threat Defense web application |
| Any (FTP client) | McAfee Advanced Threat Defense | TCP 22 (SFTP) | No | Access the FTP server on McAfee Advanced Threat Defense |
| Sensor | McAfee Advanced Threat Defense | TCP 8505 | No | Communication channel between a Sensor and McAfee Advanced Threat Defense |
| Manager | McAfee Advanced Threat Defense | TCP 443 (HTTPS) | No | Communication between the Manager and McAfee Advanced Threat Defense through the RESTful APIs. |
| McAfee Advanced Threat Defense | McAfee ePO | TCP 8443 | Yes | Host information queries. |
| McAfee Advanced Threat Defense | `tunnel.message .trustedsource.org` | TCP 443 (HTTPS) | No | File Reputation queries. |
| McAfee Advanced Threat Defense | `List.smartfilter.com` | TCP 80 (HTTP) | No | URL updates. |
| Any (SSH client) | McAfee Advanced Threat Defense | TCP 2222 (SSH) | No | CLI access |
| McAfee Advanced Threat Defense | `wpm.webwasher.com` | TCP 443 (HTTPS) | No | Updates for McAfee Gateway Anti-Malware Engine and McAfee Anti-Malware Engine. |

# Setting up McAfee Advanced Threat Defense

This chapter describes how to set up the McAfee Advanced Threat Defense Appliance for you to configure it.

**Contents**

- *Install or remove rack handles*
- *Install or remove the Appliance from the rack*
- *Turn on the McAfee Advanced Threat Defense Appliance*
- *Handling the front bezel*
- *Connect the network cable*
- *Configure network information for McAfee Advanced Threat Defense Appliance*

## Install or remove rack handles

- To install a rack handle, align it with the two holes on the side of the McAfee Advanced Threat Defense Appliance and attach the rack handle to the Appliance with two screws as shown.

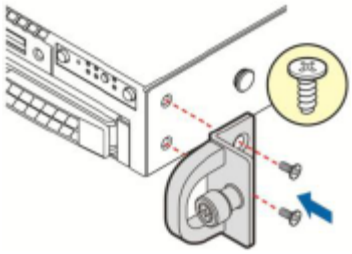


**Figure 2-6 Installing the rack handle**

- To remove a rack handle, remove the two screws holding the rack handle in place, and remove the rack handle from the server system as shown.

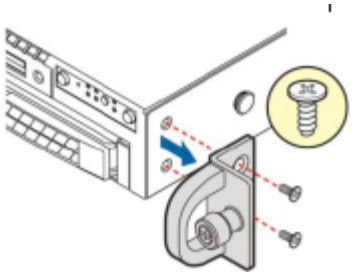


**Figure 2-7 Removing the rack handle**

## Install or remove the Appliance from the rack

Use the rack-mounting kit included with the McAfee Advanced Threat Defense Appliance to install the unit into a four-post 19-inch rack. The kit can be used with most industry-standard rack cabinets. Use the tie wraps to secure the cables from the McAfee Advanced Threat Defense Appliance to the rack.

### Task

1 At the front of the rack, position the right or the left mounting rail on the corresponding side so that its mounting bracket aligns with the required rack holes.

Ensure that you follow the safety warnings. When identifying where you want the McAfee Advanced Threat Defense Appliance to go in the rack, remember that you should always load the rack from the bottom up. If you are installing multiple McAfee Advanced Threat Defense Appliances, start with the lowest available position first.

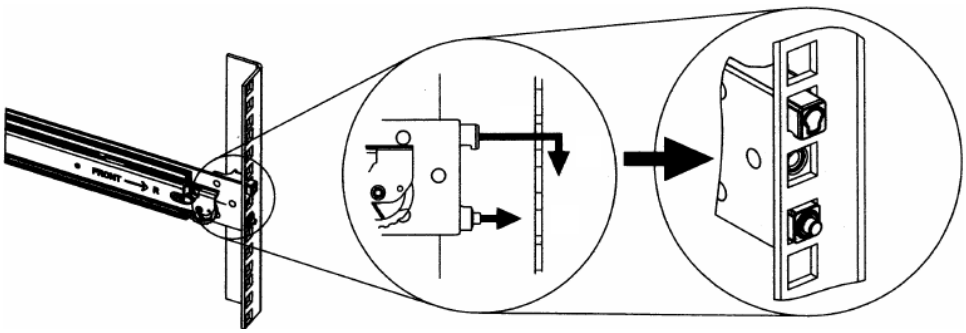


**Figure 2-8 Slide rail installation**

2 At the back of the rack, pull the back mounting-bracket (extending the mounting rail) so that it aligns with the required rack holes.

Ensure that the mounting rails are at the same level on each side of the rack.

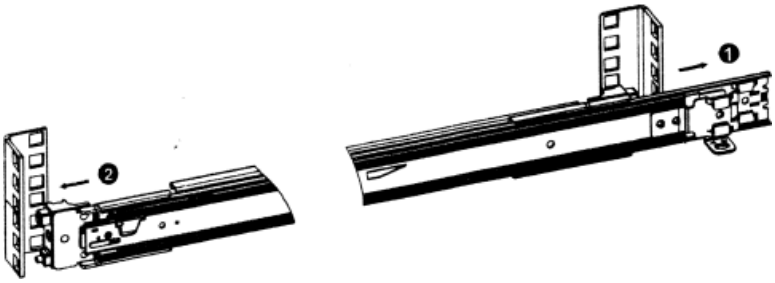


**Figure 2-9 Install rail to rack**

3 Clip the rail to the rack and secure it.

4 Repeat these steps to secure the second mounting rail to the rack.

5 Slide both the rails to full extent.

**Figure 2-10 Full extend slide**

6 With help from another person, lift the McAfee Advanced Threat Defense Appliance and install the chassis to the rail simultaneously on both the sides.

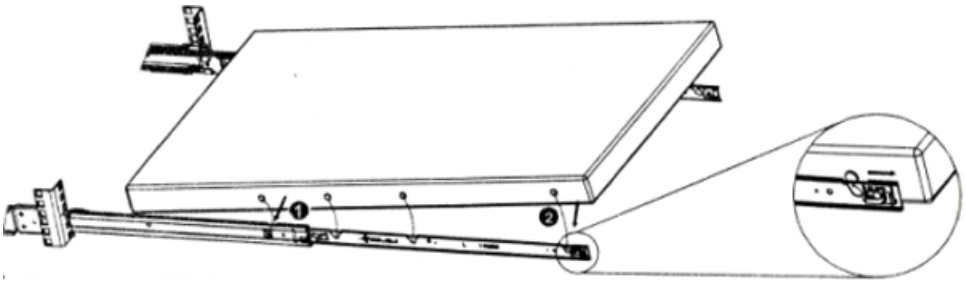


**Figure 2-11 Install the Appliance to rail**

Drop in the rear spool first, followed by the middle and then front.

Lifting the McAfee Advanced Threat Defense Appliance and attaching it to the rack is a two-person job.

7 Attach the lockable bezel to protect the front panel if required.

8 Lift the release tab and push the Appliance into the rack.

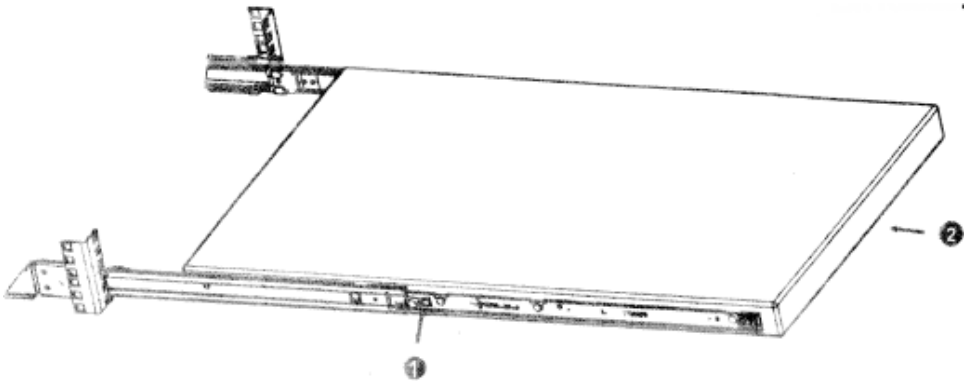



**Figure 2-12 Lift release tab and push Appliance into rack**

9 To remove the McAfee Advanced Threat Defense Appliance from the rack, lift the release tab next to the front spool on the chassis and lift it out of the rails.

This needs to be done simultaneously on both the sides and requires two people.

## Turn on the McAfee Advanced Threat Defense Appliance

The McAfee Advanced Threat Defense Appliance has redundant power supplies pre-installed.

The McAfee Advanced Threat Defense Appliance ships with two power cords specific to your country or region.

### Task

1 Plug one end of the AC power cord into the first power supply module in the back panel and the other end into an appropriate power source.

2 Plug one end of the AC power cord into the second power supply module in the back panel and the other end into an appropriate power source.

3 Push the power button on the front panel.

The on/off button on the front panel does not turn off the AC power. To remove AC power from the McAfee Advanced Threat Defense Appliance, you must unplug both AC power cords from either the power supply or wall outlet.

## Handling the front bezel

You can remove the front bezel if required, and then re-install it. However, before you install the bezel, you must install the rack handles.

### Task

1 Follow these steps to remove the front bezel.

   a Unlock the bezel if it is locked.

   b Remove the left end of front bezel from rack handle.

   c Rotate the front bezel anticlockwise to release the latches on the right end from the rack handle.

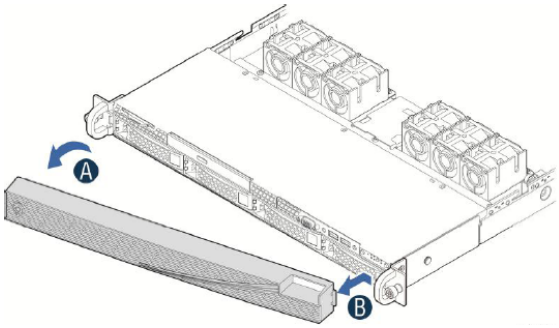



**Figure 2-13 Removing front bezel**

2 Follow these steps to install the front bezel.

   a Lock the right end of the front bezel to the rack handle

   b Rotate the front bezel clockwise until the left end clicks into place

   c Lock the bezel if needed.

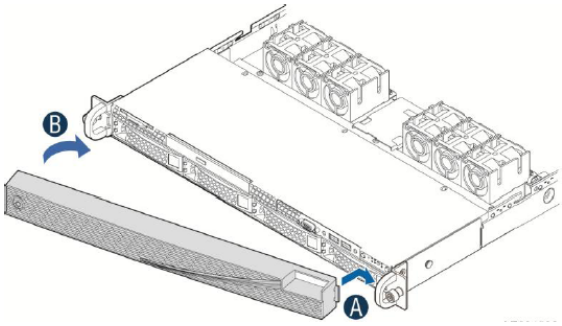



**Figure 2-14 Installing front bezel**

## Connect the network cable

### Task

1 Plug a Category 5e or 6 Ethernet cable in the management port, which is located in the back panel.

2 Plug the other end of the cable into the corresponding network device.

## Configure network information for McAfee Advanced Threat Defense Appliance

After you complete the initial installation and configuration, you can manage the McAfee Advanced Threat Defense Appliance from a remote computer or terminal server. To do so, you must configure the McAfee Advanced Threat Defense Appliance with the required network information.

## Task

1 Plug a console cable (RJ45 to DB9 serial) to the console port (RJ45 serial-A port) at the back panel of the McAfee Advanced Threat Defense Appliance.

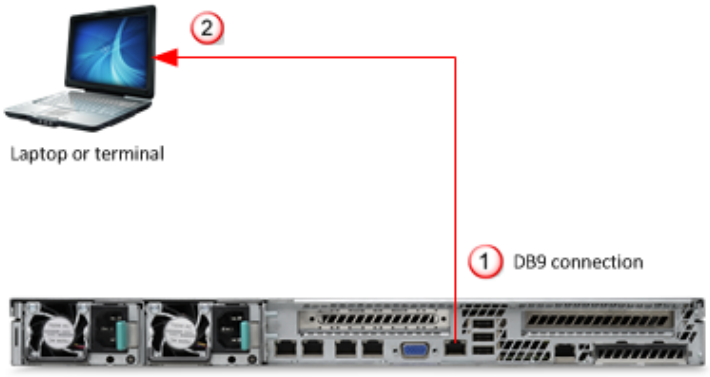



**Figure 2-15 Connect the console port**

2 Connect the other end of the cable directly to the COM port of the computer or port of the terminal server you are using to configure the McAfee Advanced Threat Defense Appliance.

3 Run the HyperTerminal from a Microsoft Windows-based computer with the following settings.

| Name | Setting |
|---|---|
| Baud rate | 115200 |
| Number of Bits | 8 |
| Parity | None |
| Stop Bits | 1 |
| Control Flow | None |

4 At the logon prompt, log on to the McAfee Advanced Threat Defense Appliance using the default user name `atdadmin` and password `atdadmin`.

You can type `help` or `?` to access instructions on using the built-in command syntax help. For a list of all commands, type `list`.

5 At the command prompt, type `set appliance name <Name>` to set the name of the McAfee Advanced Threat Defense Appliance.

You need to type the values between <> characters, excluding the <> characters.

Example: `set appliance name matd_appliance_1`

The McAfee Advanced Threat Defense Appliance name can be an alphanumeric character string up to 25 characters. The string must begin with a letter and can include hyphens, underscores, and periods, but not spaces.

6 To set the management port IP address and subnet mask of the McAfee Advanced Threat Defense Appliance, type `set appliance ip <A.B.C.D> <E.F.G.H>`

Specify a 32-bit address written as four eight-bit numbers separated by periods as in <A.B.C.D>, where A, B, C, or D is an eight-bit number between 0-255. <E.F.G.H> represents the subnet mask.

Example: `set appliance ip 192.34.2.8 255.255.255.0`

After you set the IP address the first time or when you modify the IP address, you must restart the McAfee Advanced Threat Defense Appliance.

7 Set the address of the default gateway.

`set appliance gateway <A.B.C.D>`

Use the same convention as for the `set appliance ip` command.

Example: `set appliance gateway 192.34.2.1`

8 Set the port speed and duplex settings for the management port using one of the following commands:

- `set mgmtport auto` — Sets the management port in auto mode for speed and duplex.
- `set mgmtport speed (10|100) duplex (full|half)` — Sets the speed to 10 or 100 Mbps at full or half duplex.

9 To verify the configuration, type `show`.

This displays the current configuration details.

10 To check the network connectivity, ping other network hosts. At the prompt, type `ping <IP address>`

The success message `host <ip address> is alive` appears. If the host is not reachable, `failed to talk to <ip address>` appears.

11 Change the McAfee Advanced Threat Defense Appliance password by using the `passwd` command.

A password must be between 8 and 25 characters, is case sensitive, and can consist of any alphanumeric character or symbol.

McAfee strongly recommends that you choose a password with a combination of characters that is easy for you to remember but difficult for someone else to guess.

# 3 Accessing McAfee Advanced Threat Defense web application

The McAfee Advanced Threat Defense web application is hosted on the McAfee Advanced Threat Defense Appliance. If you are a McAfee Advanced Threat Defense user with web access, you can access the McAfee Advanced Threat Defense web application from a remote machine using a supported browser.

Using the McAfee Advanced Threat Defense web application, you can:

- Monitor the state and performance of the McAfee Advanced Threat Defense Appliance.
- Manage McAfee Advanced Threat Defense users and their permissions.
- Configure McAfee Advanced Threat Defense for malware analysis.
- Manually upload files to be analyzed.
- Monitor the progress of the analysis and subsequently view the results.

**Contents**


- *McAfee Advanced Threat Defense client requirements*
- *Access the McAfee Advanced Threat Defense web application*


## McAfee Advanced Threat Defense client requirements

The following are the system requirements for client systems connecting to the McAfee Advanced Threat Defense web application.

- Client operating system —
- Browsers — Internet Explorer 9 and later, Firefox, and Chrome.

# Access the McAfee Advanced Threat Defense web application

## Task

1 From a client computer, open a session using one of the supported browsers.

2 Use the following to access the McAfee Advanced Threat Defense web application:

- URL — https://<McAfee Advanced Threat Defense appliance host name or IP address>
- Default user name — `admin`
- Password — `admin`

3 Click **Log In**.

# 4 Managing Advanced Threat Defense

You use the McAfee Advanced Threat Defense web application to manage configurations such as user accounts and to monitor the McAfee Advanced Threat Defense Appliance's system health.

**Contents**


- *Managing McAfee Advanced Threat Defense users*
- *Monitoring the McAfee Advanced Threat Defense performance*
- *Upgrade McAfee Advanced Threat Defense and Android VM*
- *Troubleshooting*
- *Backup and restore McAfee Advanced Threat Defense database*


## Managing McAfee Advanced Threat Defense users

You can create user accounts for McAfee Advanced Threat Defense with different permissions and configuration settings. These permissions and settings depend on the user's role with respect to malware analysis using McAfee Advanced Threat Defense. Using the McAfee Advanced Threat Defense web application, you can create user accounts for:

- Users who use the McAfee Advanced Threat Defense web application for submitting files for analysis and for viewing the results of the analysis.
- Users who upload the files to the FTP server hosted on the McAfee Advanced Threat Defense Appliance.
- Users who directly use the RESTful APIs for uploading files. For more information, see the *McAfee Advanced Threat Defense RESTful APIs Reference Guide.*

In the user record, you also specify the default analyzer profile. If you are using the McAfee Advanced Threat Defense web application to upload, you can override this selection when you actually upload a file.

For each user, you can also configure the FTP server details to which you want McAfee Advanced Threat Defense to upload the results of the analysis.

- There are four default user records.
  - Default admin — This is the default super-user account. You can use this account to initially configure the McAfee Advanced Threat Defense web application. The logon name is *admin* and the default password is *admin*.
  - NSP user — The logon name is *nsp* and the default password is *admin*. This is used by Network Security Platform to integrate with McAfee Advanced Threat Defense. Currently, all Network Security Platform Sensors use this user record to submit sample files.

- ATD admin — This is the default user account to access the FTP server on McAfee Advanced Threat Defense. The user name is *atdadmin* and the password is *atdadmin.*
- McAfee Web Gateway user — This is for the integration between McAfee Web Gateway and McAfee Advanced Threat Defense.

As a precaution, make sure you change the default passwords.

- To access the CLI of McAfee Advanced Threat Defense, you must use *atdadmin* as the logon name and *atdadmin* as the password. You cannot access this user record. You cannot create any other user to access the CLI.

You access the CLI through SSH over port 2222. See Log on to the CLI on page 301.

- If you are a not an admin user, you can view your user record and modify it. To modify your role assignments, you must contact the admin user.

## Viewing user profiles

If you are a user with admin role, you can view the existing list of McAfee Advanced Threat Defense users. If you do not have admin role, you can view your user record.

### Task

1 Select **Manage** | **User Management**.

The current list of users is displayed (based on your role).

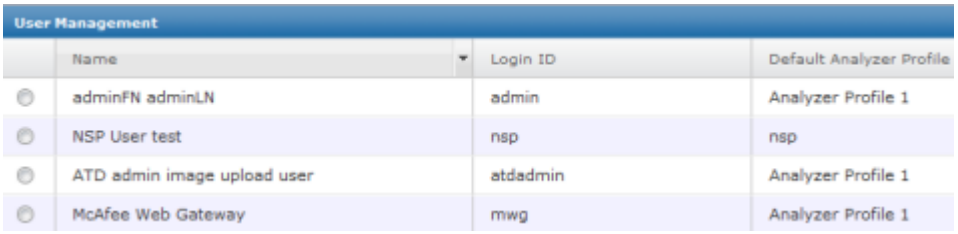



**Figure 4-1 View the list of users**

| Column name | Definition |
|---|---|
| **Select** | Select to edit or delete the user record. |
| **Name** | Full name of the user as entered in the user details. |
| **Login ID** | The user name for accessing McAfee Advanced Threat Defense. |
| **Default Analyzer Profile** | The Analyzer Profile that McAfee Advanced Threat Defense uses when the user submits a sample for analysis. However, the user can override this at the time of sample submission. |

2 Hide the columns you do not want to see.

a Move the mouse over the right corner of a column heading and click the drop-down arrow.

b Select **Columns**.

c Select only the required column names from the list.

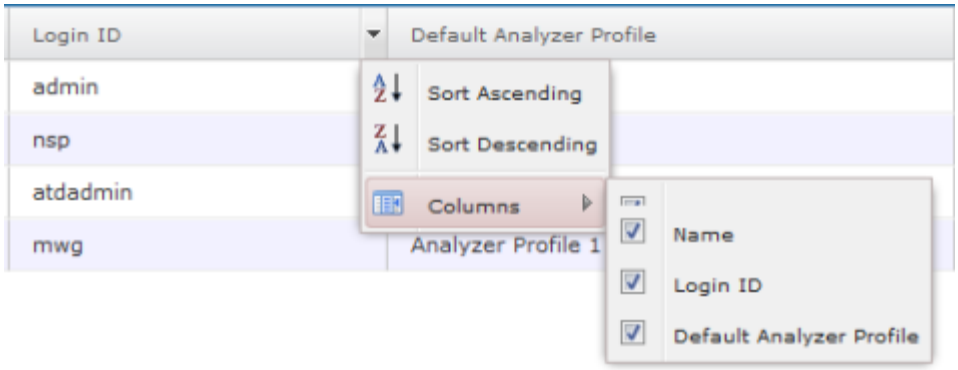



**Figure 4-2 Select the required column names**

3 To sort the user records list based on a particular column name, click the column heading.

You can sort the records in the ascending or descending order. Alternatively, move the mouse over the right corner of a column heading and click the drop-down arrow. Then select **Sort Ascending** or **Sort Descending**.

4 To view the complete details of a specific user, select the record and click **Edit**.

## Add users

If you have the *admin user* role, you can create the following types of users:

- Users with admin role in the McAfee Advanced Threat Defense web application
- Non-admin users in the McAfee Advanced Threat Defense web application
- Users with access to the FTP server hosted on the McAfee Advanced Threat Defense Appliance.
- Access to the RESTful APIs of the McAfee Advanced Threat Defense web application

## Task

1 Select **Manage** | **User Management** | **New.**

The **User Management** page is displayed.

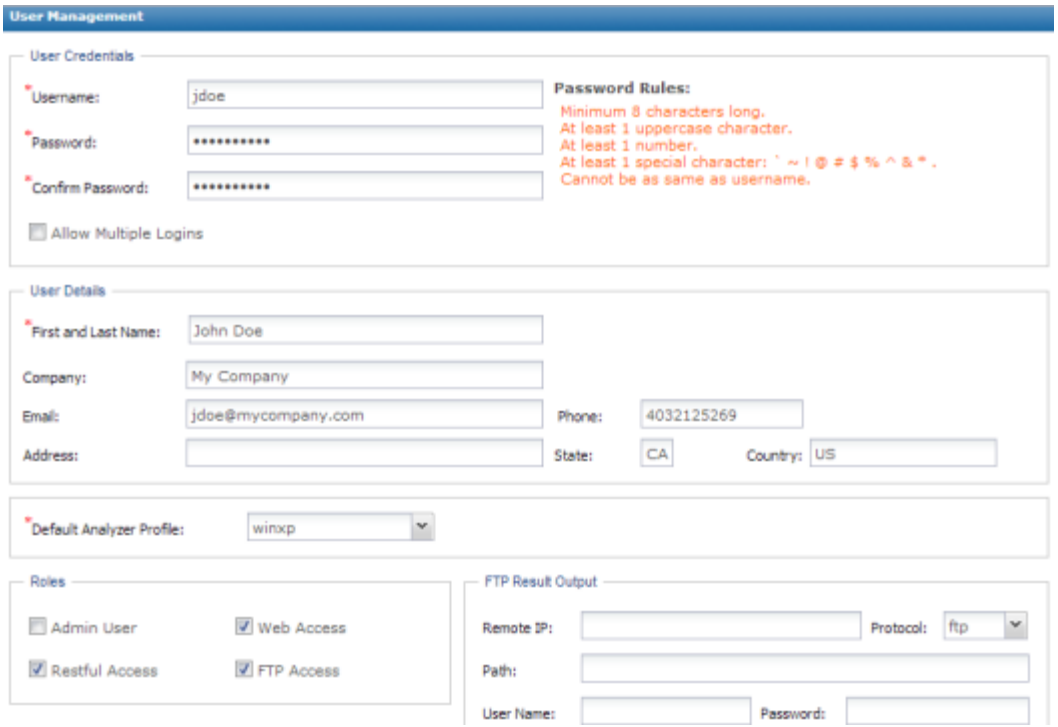



**Figure 4-3 Add users**

2 Enter the appropriate information in the respective fields.

| Option name | Definition |
|---|---|
| **Username** | The user name for accessing the McAfee Advanced Threat Defense web application, FTP server, or RESTful APIs. |
| **Password** | The default password that you want to provide to the user. It must meet the following criteria:<br>• Minimum 8 characters in length.<br>• At least one of the alphabetic characters must be in uppercase.<br>• Must contain at least 1 number.<br>• Must contain at least one of the following special characters ` ~ ! @ # $ % ^ & *<br>• Password and user name must not be same. |
| **Allow Multiple Logins** | Deselect it you want to restrict the concurrent logon sessions for this user name to just one. Select if you want to allow multiple concurrent logon sessions for the user name. |
| **First and Last Name** | Enter the full name of the user. It must be of at least 2 characters in length. |
| **Email** | Optionally, enter the email address of the user. |
| **Company** | Optionally, enter the organization to which the user belongs. |
| **Phone** | Optionally, enter the user's phone number. |

| Option name | Definition |
|---|---|
| **Address** | Optionally, enter the user's address for communication. |
| **State** | Optionally, enter the corresponding State for the address you entered. |
| **Country** | Optionally, enter the corresponding Country for the address you entered. |
| **Default Analyzer Profile** | Select the analyzer profile that must be used for files submitted by the user. For example, if Network Security Platform Sensor submits the file, the analyzer profile selected in the *NSP User* record is used.<br>Users, who manually submit files, can override this setting by selecting a different analyzer profile at the time of file submission. |
| **Roles** | • **Admin User —** Select to assign super-user rights in the McAfee Advanced Threat Defense web application. Users with this role can access all menus and create other users.<br>• **Web Access —** This role enables a user to submit files using the McAfee Advanced Threat Defense web application and view the results. Users with this role can access all features but can only view their own user profile. Also, when they manually submit files, they can assign only the analyzer profiles that they created.<br>• **FTP Access —** Select to assign access to the FTP server hosted on the McAfee Advanced Threat Defense Appliance to submit files for analysis and to upload VMDK files.<br>• **Log User Activities —** Select if you want to log the changes made by the user in the McAfee Advanced Threat Defense web application.<br>• **Restful Access —** Select to assign access to the RESTful APIs of the McAfee Advanced Threat Defense web application to submit files for analysis.<br>The **Restful Access** role must be selected for the integrated McAfee products that use RESTful APIs. If you remove this selection, the integration might not work. |
| **FTP Result Output** | Specify the details of the FTP server to which McAfee Advanced Threat Defense must provide the results of malware analysis.<br>When you configure the FTP server details, McAfee Advanced Threat Defense sends the results to the specified FTP server as well as stores in its data disk. When the data disk is 75 percent full, the older analysis results are deleted. To preserve the results for a longer term, you can configure **FTP Result Output**.<br>• **Remote IP —** The IPv4 address of the FTP server.<br>• **Protocol —** Specify whether FTP or SFTP must be used. McAfee recommends using SFTP.<br>• **Path —** The complete path to the folder where the results must be saved.<br>• **User Name —** The user name that McAfee Advanced Threat Defense must use to access the FTP server.<br>• **Password —** The password for accessing the FTP server.<br>• **Test —** to verify if McAfee Advanced Threat Defense is able to communicate with the specified FTP server using the specified protocol (FTP or SFTP). |
| **Save** | Creates the user record with the information you provided. If you configure an FTP server for result output, make sure that the test connection is successful before you click **Save**. |
| **Cancel** | Closes the **User Management** page without saving the changes. |

## Edit Users

If you are assigned the admin-user role, you can edit the user profiles. If you intend to modify the mandatory fields, then as a best practice, make sure the corresponding user is not logged on. If you are assigned only the web-access or Restful-access roles, only your user profile is available for editing.

### Task

1 Select **Manage** | **User Management**.

The current list of users is displayed.

2 Select the required user record and click **Edit**.

The **User Management** page is displayed.

3 Make the changes to the required fields and click **Save**.

For information on the fields, see Add users on page 37.

## Delete Users

If you are assigned the admin-user role, you can delete user records. Make sure that the corresponding user is not logged on.

You cannot delete any predefined user records, which are the admin user record, the user record for Network Security Platform, and the user record for McAfee Web Gateway.

### Task

1 Select **Manage** | **User Management**.

The current list of users is displayed.

2 Select the required user record and click **Delete**.

3 Click **Yes** to confirm deletion.

# Monitoring the McAfee Advanced Threat Defense performance

You can use the following options to monitor the performance of McAfee Advanced Threat Defense.

- Use the monitors on the McAfee Advanced Threat Defense dashboard to continuously monitor the performance. See McAfee Advanced Threat Defense performance monitors on page 278.
- Use the `status` command in the McAfee Advanced Threat Defense Appliance CLI. See CLI commands for McAfee Advanced Threat Defense on page 5.

# Upgrade McAfee Advanced Threat Defense and Android VM

This section provides information on how to upgrade the McAfee Advanced Threat Defense version as well as the Android version for the default Android analyzer VM.

Following are the upgrade paths to upgrade McAfee Advanced Threat Defense software to 3.2.0.xx:

- If the current version is 3.0.2.xx other than 3.0.2.36, direct upgrade to 3.2.0.xx is not supported. For example, if the current version is 3.0.2.51, first upgrade to 3.0.4.56 and then upgrade to 3.2.0.xx. Upgrade from 3.0.2.xx to 3.0.4.56 is a two-step process. See Upgrade McAfee Advanced Threat Defense software from 3.0.2.xx to 3.0.4.xx on page 41.
- If the current version is 3.0.2.36 and you want to upgrade to 3.2.0.xx, you upgrade the McAfee Advanced Threat Defense user interface and the McAfee Advanced Threat Defense system software separately. That is, direct upgrade to 3.2.0 is supported but it is a two-step process. See Upgrade McAfee Advanced Threat Defense software from 3.0.2.36 to 3.2.0.xx on page 44.
- If the current version is 3.0.4.56, 3.0.4.75, or 3.0.4.94, you can directly upgrade to 3.2.0.xx by upgrading just the McAfee Advanced Threat Defense system software. See Upgrade McAfee Advanced Threat Defense software from 3.0.4.xx to 3.2.0.xx on page 47.

Once you upgrade to 3.2.0.xx, you cannot downgrade to 3.0.2.xx or 3.0.4.xx by loading the backup image using the `reboot backup` command.

The Android version in the default Android analyzer VM is 2.3. After you upgrade McAfee Advanced Threat Defense software to 3.2.0.xx, you can upgrade the Android version to 4.3. See Upgrade the Android analyzer VM on page 49.

## Upgrade McAfee Advanced Threat Defense software from 3.0.2.xx to 3.0.4.xx

**Before you begin**

- Only if the current version of McAfee Advanced Threat Defense is 3.0.2.36, you can directly upgrade to 3.2.0. For all other 3.0.2.xx versions, first upgrade to 3.0.4.56 to upgrade to 3.2.0.xx.
- Make sure that the 3.0.4.xx McAfee Advanced Threat Defense software that you want to use is extracted and that you can access it from your client computer. The upgrade to McAfee Advanced Threat Defense 3.0.4.56 is a two-step process. You upgrade the McAfee Advanced Threat Defense user interface and the McAfee Advanced Threat Defense system software separately. Therefore, make sure that you have *ui-3.0.4.X.msu* and *system-3.0.4.x.msu* files accessible from your client computer.

  This two-step upgrade procedure applies only when you upgrade from version 3.0.2.x to 3.0.4.56. To upgrade to 3.0.4.75, first upgrade to 3.0.4.56. Then, to upgrade from 3.0.4.56 to 3.0.4.75, you only have to upgrade the McAfee Advanced Threat Defense web application user interface (MATD Software).

- You have the credentials to log on as the admin user in the McAfee Advanced Threat Defense web application.
- You have the credentials to log on to the McAfee Advanced Threat Defense CLI using SSH.
- You have the credentials to SFTP to the McAfee Advanced Threat Defense Appliance.
- For the *admin* user record, select **Allow Multiple Logins** in the **User Management** page.

Using the McAfee Advanced Threat Defense web application, you can import the McAfee Advanced Threat Defense software image that you want to upgrade to.

As a precaution, reboot the device from the active disk and use the `copyto backup` command to copy the software version from the active disk to the backup disk. With a backup, you can revert to the current software version, if necessary.

## Task

1 Upgrade the McAfee Advanced Threat Defense web application user interface.

a Select **Manage** | **Software Management**.

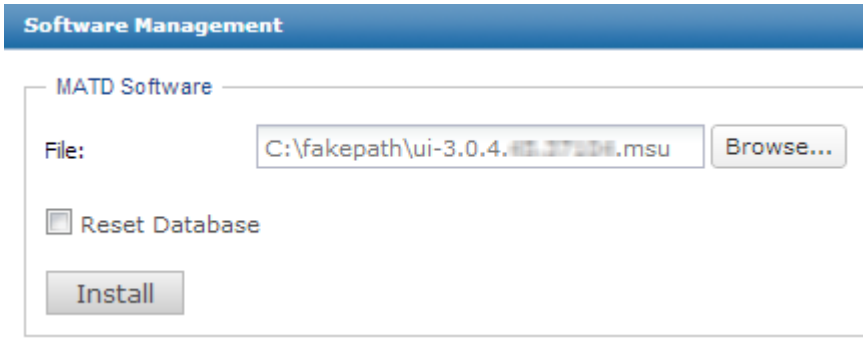



**Figure 4-4 McAfee Advanced Threat Defense web application upgrade**

b Click **Browse** and select the ui-<version number>.msu file from your client computer.

For an upgrade, make sure that **Reset Database** is deselected. You select this option only if you want a fresh database to be created as part of the upgrade. If you select this option, a warning message is displayed that all data from the existing database is lost. Click **OK** to confirm.

c Click **Install**.

d After the McAfee Advanced Threat Defense web application is upgraded, log off and then clear the cache from the corresponding browser.

e Log on to McAfee Advanced Threat Defense web application and do the following.

- Verify the version displayed in the user-interface.
- Select **Manage** | **Software Management** and verify that the **Software Management** consists of two sections — MATD Software and System Software.
- Verify the data and configurations from your earlier version are preserved.

2 Upgrade the McAfee Advanced Threat Defense system software.

a Log on to the McAfee Advanced Threat Defense Appliance using an FTP client such as FileZilla.

Log on as the atdadmin user.

b Using SFTP, upload the system-<version number>.msu file to the root directory of McAfee Advanced Threat Defense.

Make sure that the transfer mode is binary.

c After the file is uploaded, log on to the McAfee Advanced Threat Defense web application as the admin user and select **Manage** | **Software Management**.

d Under **System Software**, select the system-<version number>.msu file.

e Make sure that **Reset Database** is deselected in case of upgrades and click **Install.**

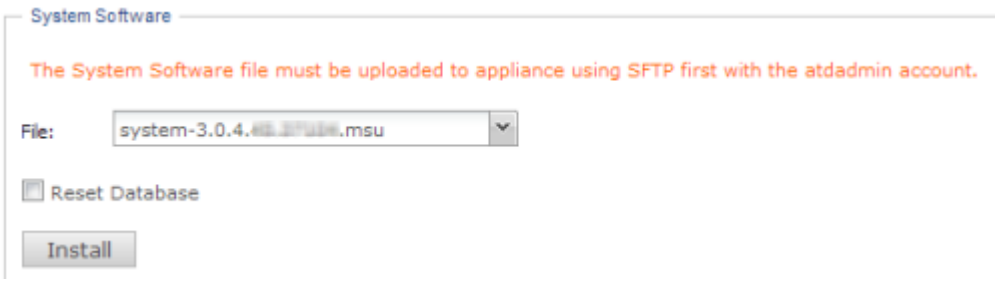
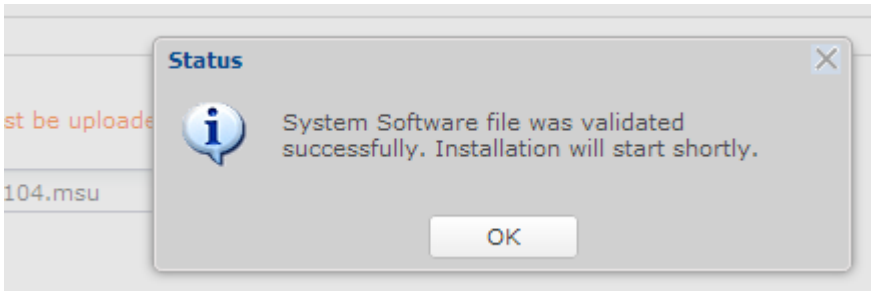
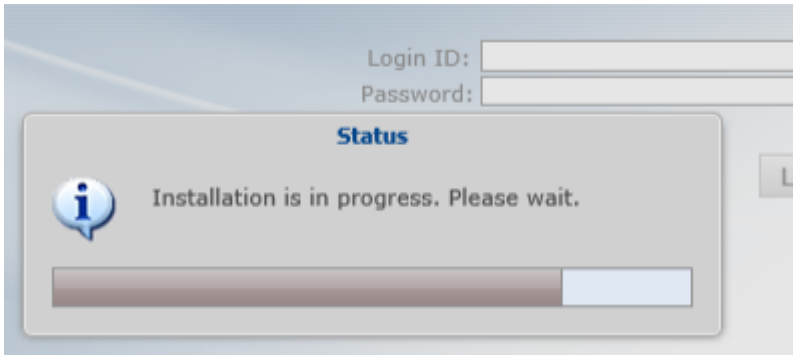



**Figure 4-5 McAfee Advanced Threat Defense web application upgrade**

f A confirmation message is displayed; click **OK**.



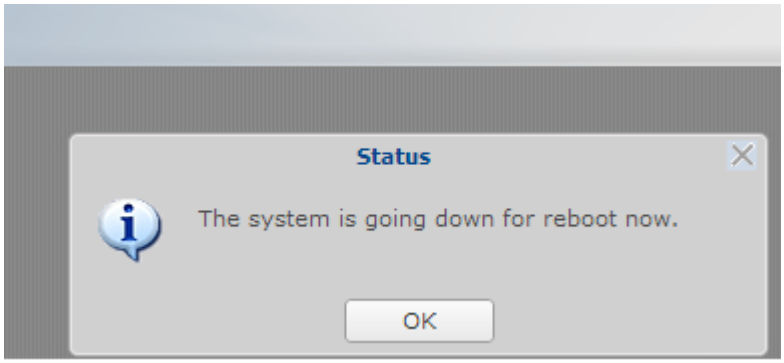

The system software is installed and the status is displayed in the browser.




It takes a minimum of 20 minutes for the system software installation to complete.

g After the software is installed McAfee Advanced Threat Defense Appliance restarts. A relevant message is displayed.

The Appliance restarts on its own. The message that is displayed is only for your information.




If you are not able to view these messages, clear the browser cache.

h Wait for McAfee Advanced Threat Defense Appliance to start. Log on to the CLI and verify the software version.

i Verify the version in the McAfee Advanced Threat Defense web application.

j Log on to the web application, and in the **System Log** page, verify that the vmcreator task is invoked.

When you upgrade to McAfee Advanced Threat Defense 3.0.4, all analyzer VMs are automatically re-created. This process might take some time to complete depending on the number of analyzer VMs.

k Verify the data and configurations from your earlier version are preserved.

The software version you upgraded to is now stored in the active disk of McAfee Advanced Threat Defense Appliance.

## Upgrade McAfee Advanced Threat Defense software from 3.0.2.36 to 3.2.0.xx

**Before you begin**

- Only if the current version of McAfee Advanced Threat Defense is 3.0.2.36, you can directly upgrade to 3.2.0. For all other 3.0.2.xx versions, first upgrade to 3.0.4.56 to upgrade to 3.2.0.xx.
- Make sure that the 3.2.0.xx McAfee Advanced Threat Defense software that you want to use is extracted and that you can access it from your client computer. The upgrade to McAfee Advanced Threat Defense 3.2.0.xx is a two-step process. You upgrade the McAfee Advanced Threat Defense user interface and the McAfee Advanced Threat Defense system software separately. Therefore, make sure that you have *ui-3.2.0.X.msu* and *system-3.2.0.x.msu* files accessible from your client computer.
- You have the credentials to log on as the admin user in the McAfee Advanced Threat Defense web application.
- You have the credentials to log on to the McAfee Advanced Threat Defense CLI using SSH.

- You have the credentials to SFTP to the McAfee Advanced Threat Defense Appliance.
- For the *admin* user record, select **Allow Multiple Logins** in the **User Management** page.

Using the McAfee Advanced Threat Defense web application, you can import the McAfee Advanced Threat Defense software image that you want to upgrade to.

## Task

1 Upgrade the McAfee Advanced Threat Defense web application user interface.

a Select **Manage** | **Software Management**.

b Click **Browse** and select the ui-3.2.0.X.msu file from your client computer.

For an upgrade, make sure that **Reset Database** is deselected. You select this option only if you want a fresh database to be created as part of the upgrade. If you select this option, a warning message is displayed that all data from the existing database is lost. Click **OK** to confirm.

c Click **Install**.

d After the McAfee Advanced Threat Defense web application is upgraded, log off and then clear the cache from the corresponding browser.

e Log on to McAfee Advanced Threat Defense web application and do the following.

- Verify the version displayed in the user-interface.
- Select **Manage** | **Software Management** and verify that the **Software Management** consists of two sections — **MATD Software** and **System Software**.
- Verify the data and configurations from your earlier version are preserved.

2 Upgrade the McAfee Advanced Threat Defense system software.

a Log on to the McAfee Advanced Threat Defense Appliance using an FTP client such as FileZilla.

Log on as the atdadmin user.

b Using SFTP, upload the system-3.2.0.x.msu file to the root directory of McAfee Advanced Threat Defense.

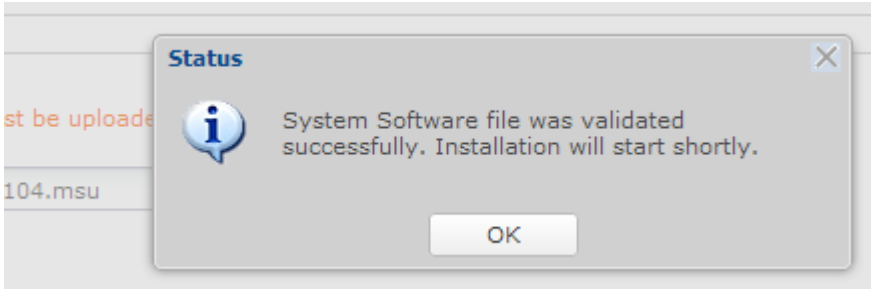
Make sure that the transfer mode is binary.

c After the file is uploaded, log on to the McAfee Advanced Threat Defense web application as the admin user and select **Manage** | **Software Management**.

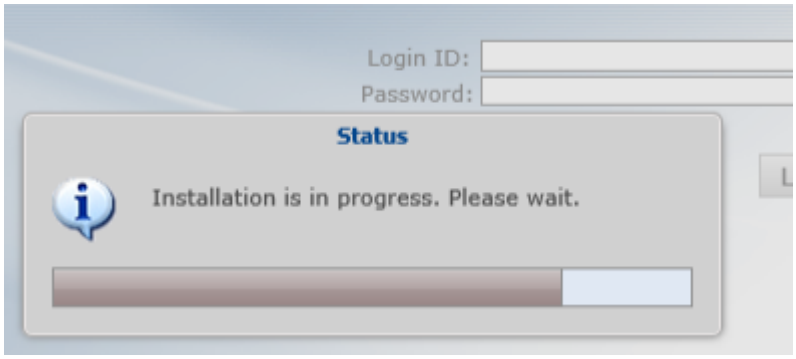
d Under **System Software**, select the system-3.2.0.x.msu file.

e Make sure that **Reset Database** is deselected in case of upgrades and click **Install**.

f A confirmation message is displayed; click **OK**.



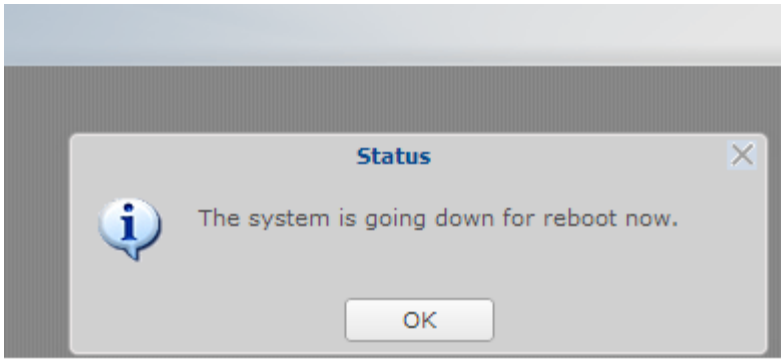

The system software is installed and the status is displayed in the browser.




It takes a minimum of 20 minutes for the system software installation to complete.

g After the software is installed McAfee Advanced Threat Defense Appliance restarts. A relevant message is displayed.

The Appliance restarts on its own. The message that is displayed is only for your information.




If you are not able to view these messages, clear the browser cache.

h Wait for McAfee Advanced Threat Defense Appliance to start. Log on to the CLI and verify the software version.

i Verify the version in the McAfee Advanced Threat Defense web application.

j Log on to the web application, and in the **System Log** page, verify that the vmcreator task is invoked.

When you upgrade to McAfee Advanced Threat Defense 3.2.0, all analyzer VMs are automatically re-created. This process might take some time to complete depending on the number of analyzer VMs.

k Verify the data and configurations from your earlier version are preserved.

The software version you upgraded to is now stored in the active disk of McAfee Advanced Threat Defense Appliance.

## Upgrade McAfee Advanced Threat Defense software from 3.0.4.xx to 3.2.0.xx

**Before you begin**

- Make sure that the current version of McAfee Advanced Threat Defense is 3.0.4.56, 3.0.4.75, or 3.0.4.94. If the current version is 3.0.2.xx, see the corresponding section for upgrade information.
- Make sure that the *system-3.2.0.x.msu* McAfee Advanced Threat Defense software that you want to use is extracted and that you can access it from your client computer.
- You have the credentials to log on as the admin user in the McAfee Advanced Threat Defense web application.
- You have the credentials to log on to the McAfee Advanced Threat Defense CLI using SSH.
- You have the credentials to SFTP to the McAfee Advanced Threat Defense Appliance.
- For the *admin* user record, select **Allow Multiple Logins** in the **User Management** page.

Using the McAfee Advanced Threat Defense web application, you can import the McAfee Advanced Threat Defense software image that you want to upgrade to.

### Task

1 Log on to the McAfee Advanced Threat Defense Appliance using an FTP client such as FileZilla.

Log on as the atdadmin user.

2 Using SFTP, upload the system-<version number>.msu file to the root directory of McAfee Advanced Threat Defense.

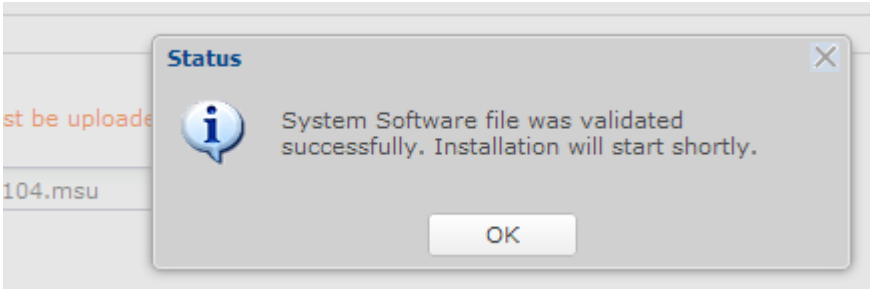
Make sure that the transfer mode is binary.

3 After the file is uploaded, log on to the McAfee Advanced Threat Defense web application as the admin user and select **Manage** | **Software Management**.

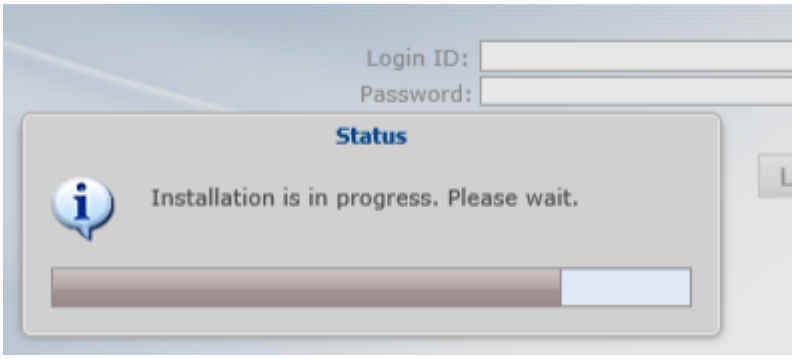
4 Under **System Software**, select the system-<version number>.msu file.

5 Make sure that **Reset Database** is deselected in case of upgrades and click **Install**.

6 A confirmation message is displayed; click **OK**.



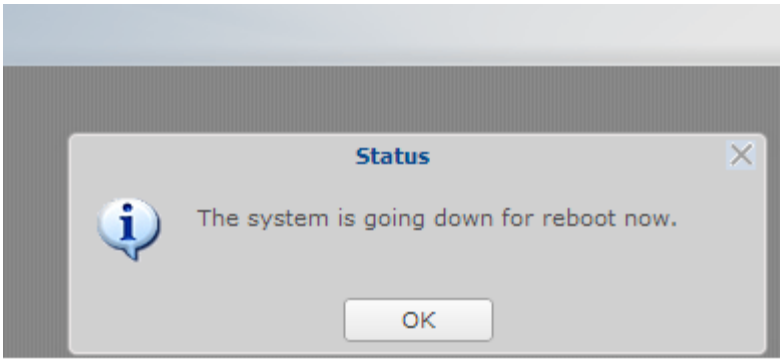

The system software is installed and the status is displayed in the browser.




It takes a minimum of 20 minutes for the system software installation to complete.

7 After the software is installed McAfee Advanced Threat Defense Appliance restarts. A relevant message is displayed.

The Appliance restarts on its own. The message that is displayed is only for your information.




If you are not able to view these messages, clear the browser cache.

8 Wait for McAfee Advanced Threat Defense Appliance to start. Log on to the CLI and verify the software version.

9 Verify the version in the McAfee Advanced Threat Defense web application.

10 Log on to the web application, and in the **System Log** page, verify that the vmcreator task is invoked.

When you upgrade to McAfee Advanced Threat Defense 3.2.0, all analyzer VMs are automatically re-created. This process might take some time to complete depending on the number of analyzer VMs.

11 Verify the data and configurations from your earlier version are preserved.

The software version you upgraded to is now stored in the active disk of McAfee Advanced Threat Defense Appliance.

## Upgrade the Android analyzer VM

**Before you begin**

- Make sure that the current version of McAfee Advanced Threat Defense is 3.2.0.xx
- Make sure that the *android-4.3.msu* is extracted and that you can access it from your client computer.
- You have the credentials to log on as the admin user in the McAfee Advanced Threat Defense web application.
- You have the credentials to log on to the McAfee Advanced Threat Defense CLI using SSH.
- You have the credentials to SFTP to the McAfee Advanced Threat Defense Appliance.
- For the *admin* user record, select **Allow Multiple Logins** in the **User Management** page.

Using the McAfee Advanced Threat Defense web application, you can upgrade the Android analyzer VM to version 4.3.

### Task

1 Log on to the McAfee Advanced Threat Defense Appliance using an FTP client such as FileZilla.

Log on as the atdadmin user.

2 Using SFTP, upload the *android-4.3.msu* file to the root directory of McAfee Advanced Threat Defense.

Make sure that the transfer mode is binary.

3 After the file is uploaded, log on to the McAfee Advanced Threat Defense web application as the admin user and select **Manage** | **Software Management**.

4 Under **System Software**, select the *android-4.3.msu* file.

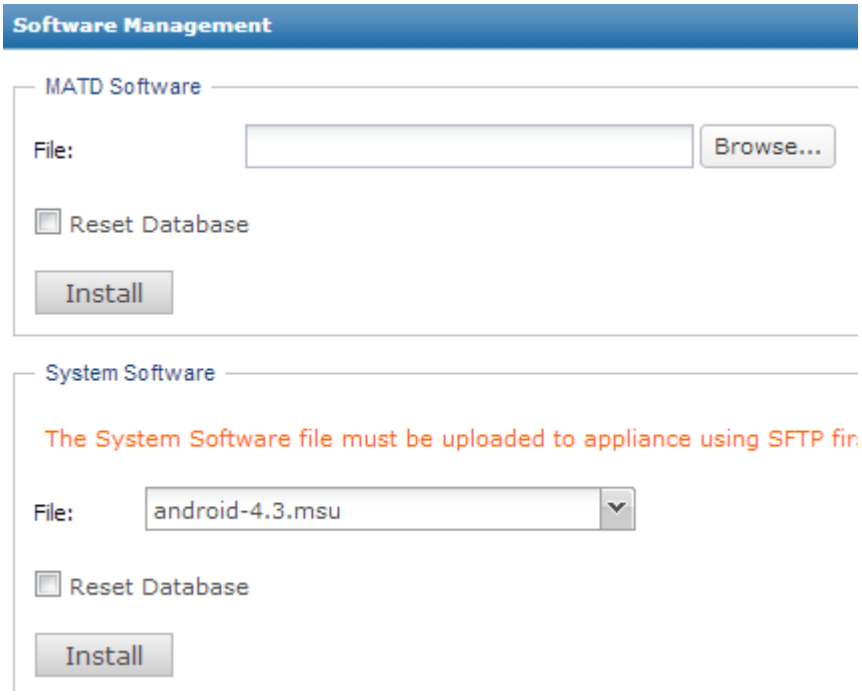
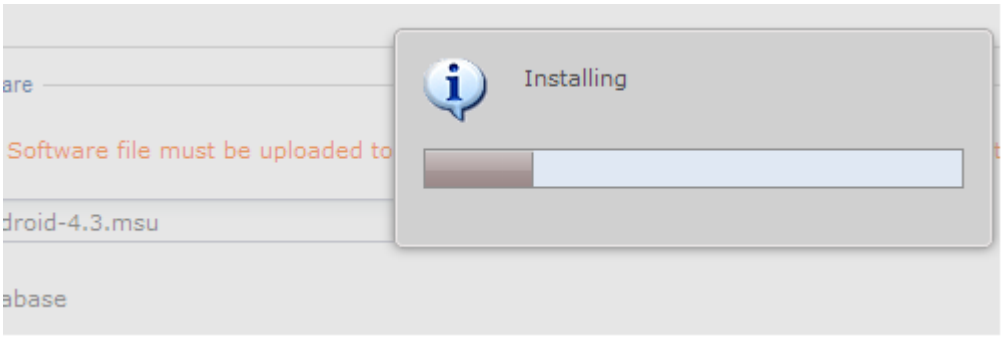
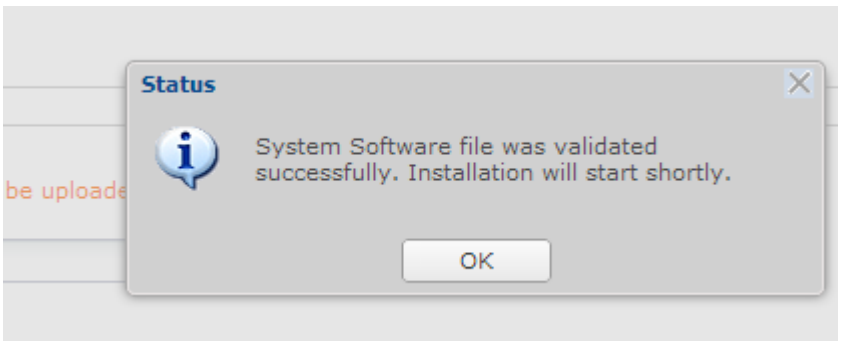



**Figure 4-6 Select the Android file**

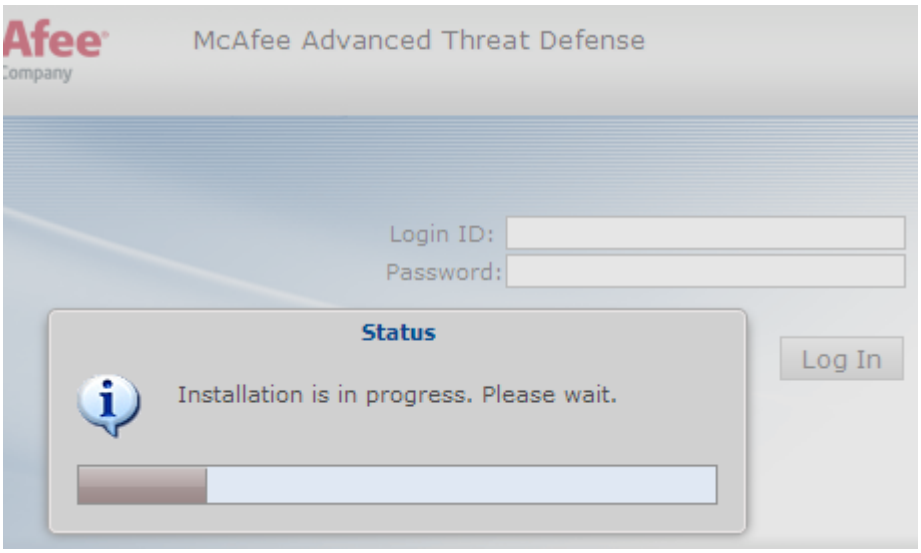
5 Make sure that **Reset Database** is deselected as this is not relevant for Android upgrade and click **Install**. Android installation process begins with file validation.




6 A confirmation message is displayed; click **OK**.



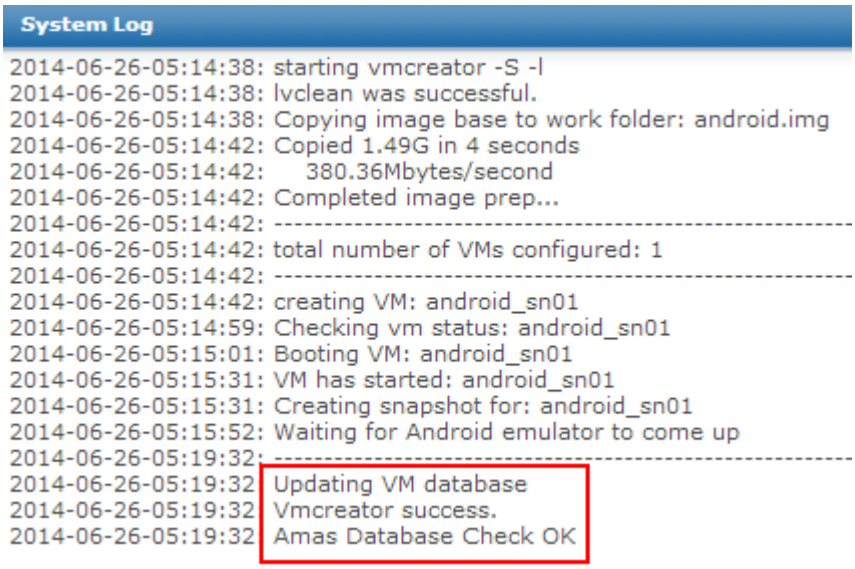
McAfee Advanced Threat Defense web application closes logs out automatically and the status of the installation is displayed in the browser.




- It takes a minimum of 20 minutes for the system software installation to complete.
- If you are not able to view these messages, clear the browser cache.
- When you upgrade Android, the default Android analyzer VM is automatically re-created. This process might take a few minutes to complete.

7 Log on to the web application, and select **Manage** | **System Log**.

8 In the **System Log** page, verify that the vmcreator task is successfully completed for the Android analyzer VM.


System Log
2014-06-26-05:14:38: starting vmcreator -S -l
2014-06-26-05:14:38: lvclean was successful.
2014-06-26-05:14:38: Copying image base to work folder: android.img
2014-06-26-05:14:42: Copied 1.49G in 4 seconds
2014-06-26-05:14:42: 380.36Mbytes/second
2014-06-26-05:14:42: Completed image prep...
2014-06-26-05:14:42: ----------
2014-06-26-05:14:42: total number of VMs configured: 1
2014-06-26-05:14:42: ----------
2014-06-26-05:14:42: creating VM: android_sn01
2014-06-26-05:14:59: Checking vm status: android_sn01
2014-06-26-05:15:01: Booting VM: android_sn01
2014-06-26-05:15:31: VM has started: android_sn01
2014-06-26-05:15:31: Creating snapshot for: android_sn01
2014-06-26-05:15:52: Waiting for Android emulator to come up
2014-06-26-05:19:32: ----------
2014-06-26-05:19:32 Updating VM database
2014-06-26-05:19:32 Vmcreator success.
2014-06-26-05:19:32 Amas Database Check OK

# Troubleshooting

The **Troubleshooting** page enables you to complete some tasks related to troubleshooting McAfee Advanced Threat Defense web application. These include exporting logs from McAfee Advanced Threat Defense and clear all the stored analysis results from the McAfee Advanced Threat Defense database.

### Task

- To access the **Troubleshooting** page, select **Manage** | **Troubleshooting**.

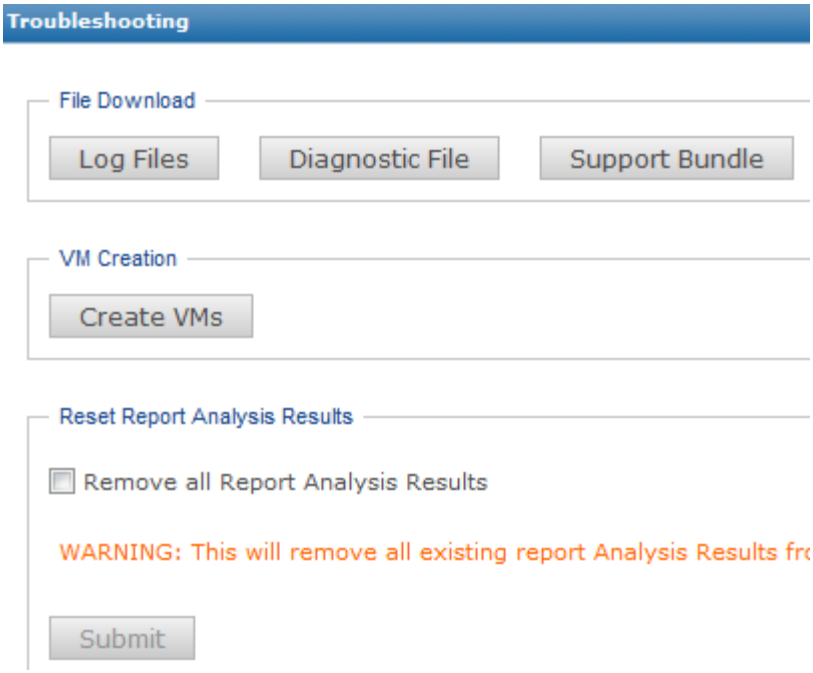



**Figure 4-7 Troubleshooting page**

### Tasks

- *Export McAfee Advanced Threat Defense logs* on page 52
- *Recreate the analyzer VMs* on page 53
- *Delete the analysis results* on page 54

## Export McAfee Advanced Threat Defense logs

If you face issues using McAfee Advanced Threat Defense, you can export the log files and provide them to McAfee support for analysis and troubleshooting. You can export system logs, diagnostic logs, and additional miscellaneous logs. The system logs help to troubleshoot issues related to features, operations, events, and so on. The diagnostic logs are needed to troubleshoot critical issues such as system crashes in McAfee Advanced Threat Defense.

You cannot read the contents of system or diagnostic log files. All these logs are intended for McAfee support.

### Task

1 In the **Troubleshooting** page, click **Log files** to download the system logs and **Diagnostic File** to download the diagnostic logs.

2 To download the additional miscellaneous information and logs, click **Support Bundle**, enter the ticket number, and click **OK**.

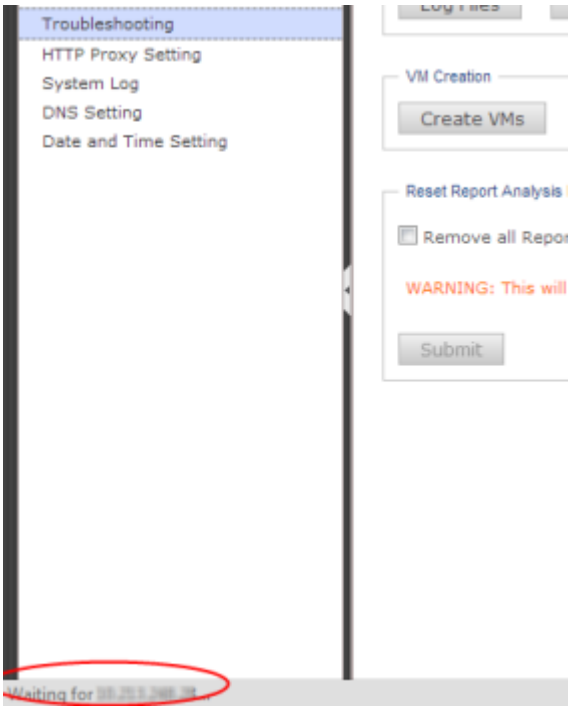



**Figure 4-8 Support bundle creation**

McAfee Advanced Threat Defense collects the required information and a message is displayed at the bottom of the browser. After some time, option to save the <ticket number>.tgz file is provided.

3 Provide the following files to McAfee support.

- System logs (atdlogs.bin)
- Diagnostic logs (atdcore.bin)
- Additional miscellaneous logs (<ticket number>.tgz)

## Recreate the analyzer VMs

During dynamic analysis, samples might corrupt some of the analyzer VMs. So, these analyzer VM instances might not be available for further analysis. Under such circumstances, you can delete all the existing analyzer VMs and recreate them.

All the existing analyzer VMs including the default Android VM and also the healthy analyzer VMs are deleted and re-created. So, no file analysis is possible until all the analyzer VMs are created again. The time taken for the re-creation varies based on the number of analyzer VM instances as well as their size.

### Task

1 In the **Troubleshooting** page, click **Create VMs** and confirm that you want to delete all existing analyzer VM instances and recreate them.

2 Select **Manage** | **System Log** to view the logs related to VM re-creation.

You can select **Dashboard** and view the **VM Creation Status** monitor to know the progress of VM re-creation. The **Create VMs** button in the **Troubleshooting** page is available again only after all the analyzer VM instances have been re-created.

## Delete the analysis results

### Task

- In the **Troubleshooting** page, click **Remove all Report Analysis Results** and click **Submit**.

# Backup and restore McAfee Advanced Threat Defense database

As a precautionary method, you can periodically take a backup of the McAfee Advanced Threat Defense database. You can then restore a backup of your choice when required. For example, if you want to discard all changes made during a troubleshooting exercise, you can restore the backup that was taken before you started troubleshooting.

Using the McAfee Advanced Threat Defense web application, you can schedule automatic backups on a daily, weekly, or monthly basis. Also specify the FTP server details, where you want McAfee Advanced Threat Defense to store the backup files. At the scheduled time, McAfee Advanced Threat Defense takes a backup of the database and sends it to the configured FTP server using FTP or SFTP according to your configuration.

When you want to restore a backup, McAfee Advanced Threat Defense fetches the selected backup file from the FTP server and overwrites its database with the contents of the backup file.

The backup and restore feature is configurable exclusively for each admin user of McAfee Advanced Threat Defense web application. Suppose that John and Mercy are admin users. Both of them can schedule backups at different times and also specify different FTP servers for storing the backups. However, if the FTP servers are different, John cannot restore a backup from Mercy's FTP server.

### What gets backed up?

The following data gets backed up:

- The analysis results as displayed in the **Analysis Results** page is backed up. However, the analysis reports such as the analysis summary, complete results, and disassembly results are not backed up. So, if you delete the reports from the database (from the **Troubleshooting page** ) and then restore a backup, the result details are listed in the **Analysis Results** page from the backup, but the reports are not available.
- Local blacklist (local whitelist is not backed up).
- VM profiles are backed up. However, the image or VMDK file of the analyzer VMs are not backed up. So, before you restore a backup, make sure the image files specified in the backed-up VM profiles are present in McAfee Advanced Threat Defense.
- Analyzer profiles.
- User records.

- McAfee ePO integration details.
- HTTP proxy settings
- DNS settings
- Date and time settings including the NTP server details.
- Load-balancing cluster settings as displayed in the **Load Balancing Cluster Setting** page. This does not include the configuration and analysis results from the other nodes in the cluster.
- Custom YARA rules and configuration
- Backup scheduler settings
- Backed up file details as displayed in the **Restore Management** page.

The following data do not get backed up:

- Any sample file or URL that is being analyzed at the time of backup. So, the **Analysis Status** page shows that the file being currently analyzed only.
- The VMDK or image files of analyzer VMs.
- The McAfee Advanced Threat Defense software in the active or backup disk.
- The log files and diagnostic files.

## Schedule a database backup

**Before you begin**

- You have admin rights in McAfee Advanced Threat Defense web application.
- You have configured an FTP server for storing the backups and you are aware of the directory in which you want to store the backups.
- You have IPv4 address of the FTP server, user name, and password for McAfee Advanced Threat Defense to access that FTP server. Also, the user name has write access to the directory that you plan to use.
- Communication over SFTP or FTP is possible between McAfee Advanced Threat Defense and the FTP server.

You can schedule automatic backup on a daily, weekly, or monthly frequency. The time taken for the backup process to complete is usually a few minutes. However, it varies based on the size of the data involved. McAfee recommends that you choose a time when the analysis load on the McAfee Advanced Threat Defense is likely to be less.

Because the backup feature is configurable for each admin user, the FTP server settings in the **Backup Scheduler Setting** page and the **FTP Result Output** settings in the **User Management** page for an admin user are the same. So, when an admin user modifies the FTP details in one of those pages, it automatically reflects in the other page.

## Task

1 Select **Manage** | **Backup and Restore** | **Backup.**

The **Backup Scheduler Setting** page is displayed.

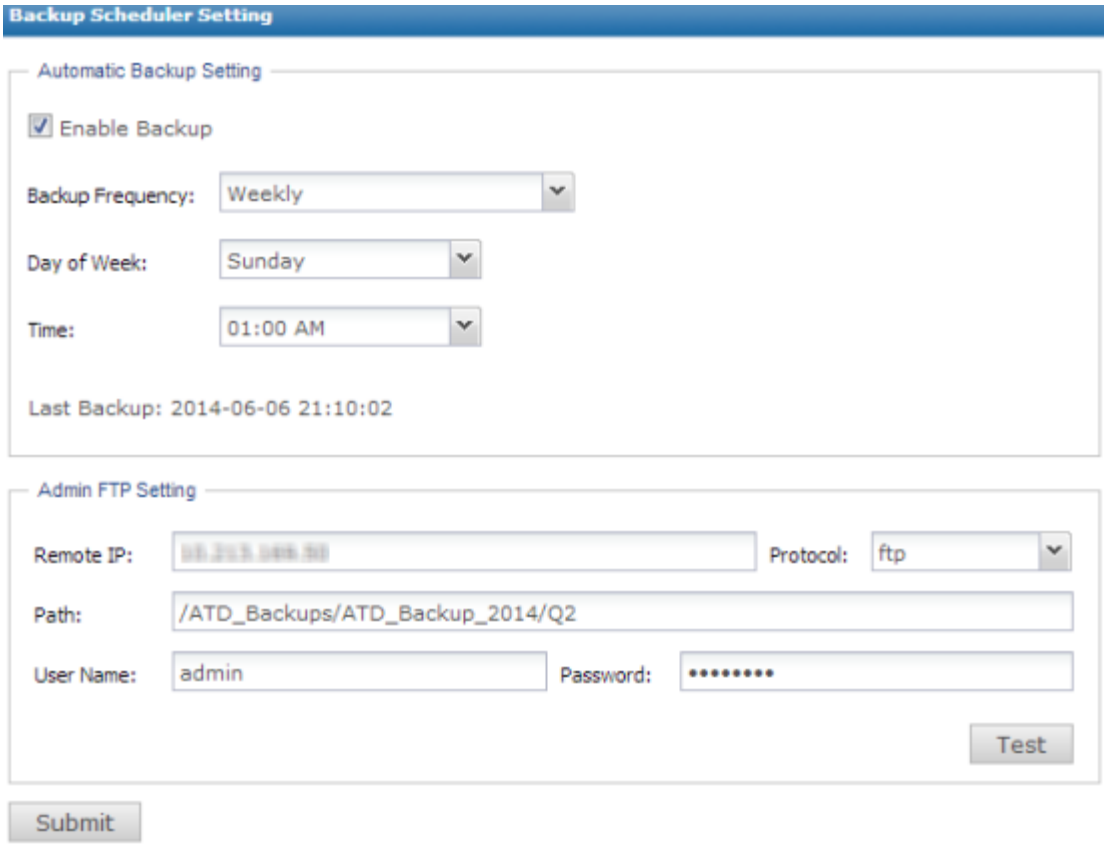



**Figure 4-9 Schedule a backup**

2 Enter the appropriate information in the respective fields.

The FTP configuration in the **Backup Scheduler Setting** page is the same as that of

| Option name | Definition |
|---|---|
| **Enable Backup** | Select to enable automatic backup at the scheduled time. If you want to stop the automatic backup, deselect this checkbox. |
| **Backup Frequency** | Specify how frequent you want McAfee Advanced Threat Defense to back up the database.<br>• **Daily** — Select to backup daily.<br>**Time** — Specify the time for the daily backup. For example, if you select 1 a.m, McAfee Advanced Threat Defense backs up at 1 a.m. daily according to its clock.<br> To back up immediately, you can use the `show` command on the McAfee Advanced Threat Defense CLI to know the current time on McAfee Advanced Threat Defense. Then with **Daily** as the backup frequency, you can specify a time accordingly to back up immediately.<br>• **Weekly** — Select to backup once a week.<br>• **Day of the week** — Select the day when you want to back up.<br>• **Time** — Specify the time of the backup on the selected day.<br>• **Monthly** — Select to backup once a month.<br>• **Day of Month** — Select the date when you want to back up. For example, if you select 5, McAfee Advanced Threat Defense backs up the database on the fifth of every month. You can only specify a date up to 28. This avoids invalid dates such as February thirtieth.<br>• **Time** — Specify the time of the backup on the selected date. |
| **Last Backup** | Timestamp of the last successful backup. |
| **Remote IP** | The IPv4 address of the FTP server. |
| **Protocol** | Select if you want to McAfee Advanced Threat Defense to use FTP or SFTP to transfer the backup file to the FTP server. |
| **Path** | The directory where McAfee Advanced Threat Defense must save the file on the FTP server. For example, to save the file at the root directory, enter / |
| **User Name** | The user name that McAfee Advanced Threat Defense must use to access the FTP server. Make sure that this user name has write access to the specified folder. |
| **Password** | The corresponding password. |
| **Test** | Click to make sure that McAfee Advanced Threat Defense is able to access the specified FTP server using the selected protocol and user credentials.<br> You can schedule a backup successfully only if the test connection succeeds. |
| **Submit** | Click to schedule the backup. |

3 To view the logs related to backup, select **Manage** | **System Log** to view the details such as the start and end timestamps.

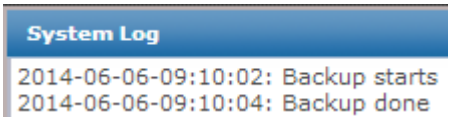



**Figure 4-10 Logs related to backup**

The backup is stored in a password-protected .zip file in the specified directory in the FTP server.

Do not try to unzip or tamper with this file. If the file gets corrupted, you might not be able to restore the database backup using that file.

## Restore a database backup

**Before you begin**

- You configured the FTP IP address, directory path, and user credentials in the **Backup Scheduler Setting** page and the test connection is working for the specified configuration. You can restore a backup only from the same FTP server that you used for taking the backup.
- The corresponding backup file that you plan to restore is available on the FTP server at the specified directory.
- As a precaution, make sure that there is no other user logged on to McAfee Advanced Threat Defense during the restoration window. Factor in the McAfee Advanced Threat Defense web application, REST APIs, and CLI.
- Make sure that McAfee Advanced Threat Defense is not analyzing any sample files or URLs at the time of restoration. Also, make sure no integrated product, user, or script is submitting samples during the restoration window.
- Make sure that you do not restore a backup during the backup window.
- Make sure that there is no McAfee Advanced Threat Defense software upgrade happening during the restoration window.

The time taken for the backup restore process to complete is usually a few minutes. However, it varies based on the size of the data involved.

- You can only restore a backup on the same McAfee Advanced Threat Defense Appliance from which the database was backed up. For example, you cannot restore a backup from a test McAfee Advanced Threat Defense Appliance onto a production McAfee Advanced Threat Defense Appliance.
- To restore the backup, the McAfee Advanced Threat Defense software version must exactly match. For example, you cannot restore a backup from an earlier or later version. Also, all numbers in the version must exactly match. For example, you cannot restore a backup from 3.0.4.94.39030 on 3.0.4.94.39031.

There could be some changes regarding the FTP server used for the backup. For example, the IP address of the FTP backup server could change or you might want to migrate the FTP server to a new physical or virtual server. If the IP address changes, make sure you update the configuration accordingly in the **Backup Scheduler Setting** page. You can then restore from the required backup file. However, if the server itself is changed, you cannot restore the backups stored in the old server. You can only restore from the files backed up in the new server.

## Task

1 Select **Manage** | **Backup and Restore** | **Restore**

The **Restore Management** page is displayed.

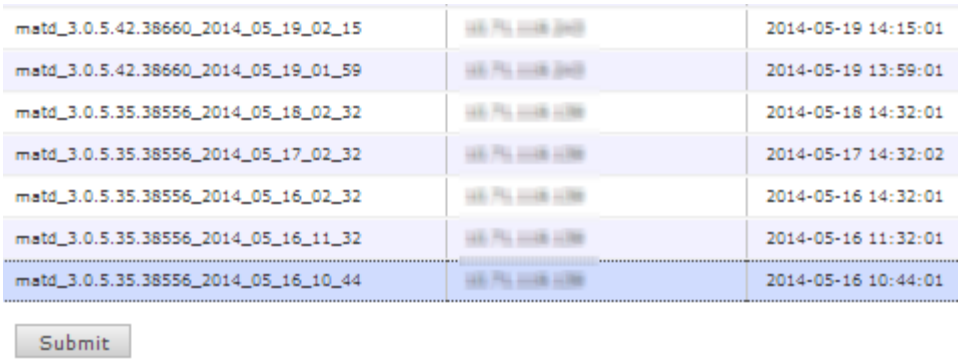



**Figure 4-11 List of available backup files**

| Option name | Definition |
|---|---|
| **File Name** | The name, which McAfee Advanced Threat Defense assigned to the backup file.<br>Do not attempt to change the file name in the FTP server. |
| **Backup Server IP Address** | The IP address of the FTP server in which the backup files are stored. |
| **Backup Time** | Timestamp of when the backup was taken. |
| **Remote IP** | The IPv4 address of the FTP server. |
| **Submit** | Select the required backup file and click **Submit** to restore the data from that backup file.<br>Restoration fails if the backup file is not available at the specified location on the backup server. |

2 To view the logs related to restore, select **Manage** | **System Log**.

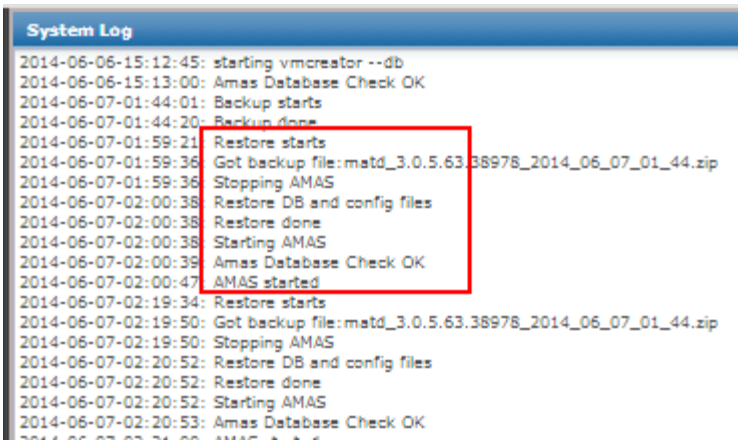



**Figure 4-12 Logs related to data restore**

The processes related to sample analysis are stopped before the restore process and restarted after the restore process.

# 5 Creating analyzer VM

For dynamic analysis, McAfee Advanced Threat Defense executes a suspicious file in a secure virtual machine (VM) and monitors its behavior for malicious activities. This VM is referred to as an analyzer VM. This chapter provides the steps for creating an analyzer VM and the VM profile.

Any security software or low-level utility tool on an analyzer VM, might interfere with the dynamic analysis of the sample file. The sample-file execution might itself be terminated during dynamic analysis. As a result, the reports might not capture the full behavior of the sample file. If you need to find out the complete behavior of a sample file, do not patch the operating system of the analyzer VM or install any security software on it. If you need to find out the effect of the sample file specific to your network, use your Common Operating Environment (COE) image, with the regular security software, to create the analyzer VMs.

The high-level steps for creating an analyzer VM and the VM profile are as follows:

1 Create an ISO image of the corresponding operating system. You must also have the license key for that operating system. For example, to create an Windows 7 analyzer VM, you must have an ISO image of Windows 7 and the license key.

   Only the following operating systems are supported to create the analyzer VMs:

   - Microsoft Windows XP 32-bit Service Pack 2
   - Microsoft Windows XP 32-bit Service Pack 3
   - Microsoft Windows Server 2003 32-bit Service Pack 1
   - Microsoft Windows Server 2003 32-bit Service Pack 2
   - Microsoft Windows Server 2008 R2 Service Pack 1
   - Microsoft Windows 7 32-bit Service Pack 1
   - Microsoft Windows 7 64-bit Service Pack 1
   - Microsoft Windows 8.0 Pro 32-bit
   - Microsoft Windows 8.0 Pro 64-bit
   - Android 2.3 by default. You can upgrade it to Android 4.3. See Upgrade the Android analyzer VM on page 49.

   All of the above Windows operating systems can be in English, Chinese Simplified, Japanese, German, or Italian.

   The only pre-installed analyzer VM is the Android VM.

2 Using VMware Workstation 9.0, create a Virtual Machine Disk (VMDK) file of the ISO image. After you create the VM, you can install the required applications such as:
   - Internet Explorer versions 6, 7, 8, 9, and 10.
   - Firefox versions 11, 12, and 13.
   - Microsoft Office versions 2003, 2007, 2010, or 2013.
   - Adobe Reader version 8, 9, or 10.
3 Import the VMDK file into the McAfee Advanced Threat Defense Appliance.
4 Convert the VMDK file into an image (.img) file.
5 Create the VM and the VM profile.

If you already have a VMDK file, it must be a single file that contains all the files required to create the VM.

**Contents**


- *Create a VMDK file for Windows XP*
- *Create a VMDK file for Windows 2003 Server*
- *Create a VMDK file for Windows 7*
- *Create a VMDK file for Windows 2008 Server*
- *Create a VMDK file for Windows 8*
- *Import a VMDK file into McAfee Advanced Threat Defense*
- *Convert the VMDK file to an image file*
- *Managing VM profiles*
- *View the VM creation log*


# Create a VMDK file for Windows XP

**Before you begin**

- Download VMware Workstation 9.0 or above from http://www.vmware.com/products/workstation/workstation-evaluation and install it.
- Make sure you have the ISO image of the operating system whose VMDK file you need to create.
- Make sure you have the license key for the operating system.

**Table 5-1 Create a VMDK file from Windows XP SP2 or SP3 ISO image.**

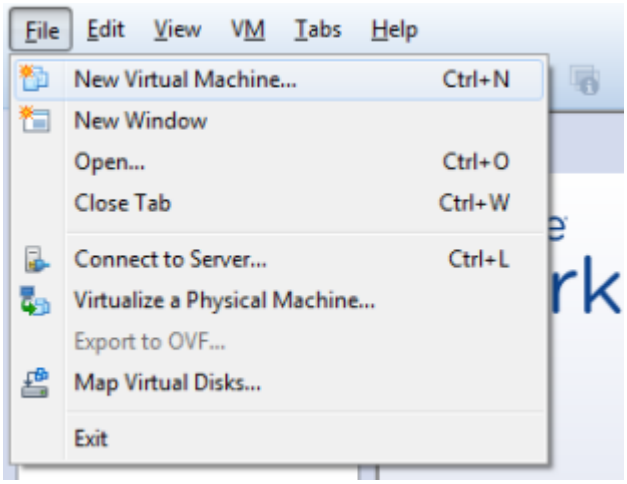
| Step | Details |
|---|---|
| **Step 1:** Start the VMware Workstation. | This procedure uses VMware Workstation 10 as an example. |
| **Step 2:** In the VMware Workstation page, select **File** \| **New Virtual Machine.** |  |
| **Step 3:** In the **New Virtual Machine Wizard** window, select **Custom (Advanced)** and click **Next.** | |

**Table 5-1 Create a VMDK file from Windows XP SP2 or SP3 ISO image.** *(continued)*

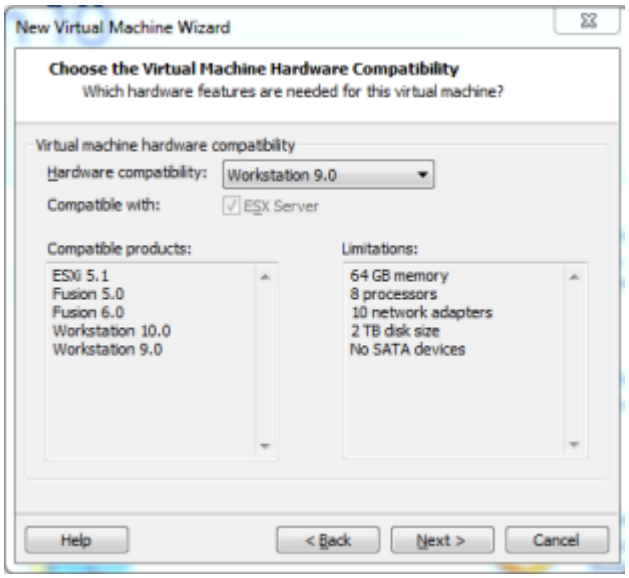
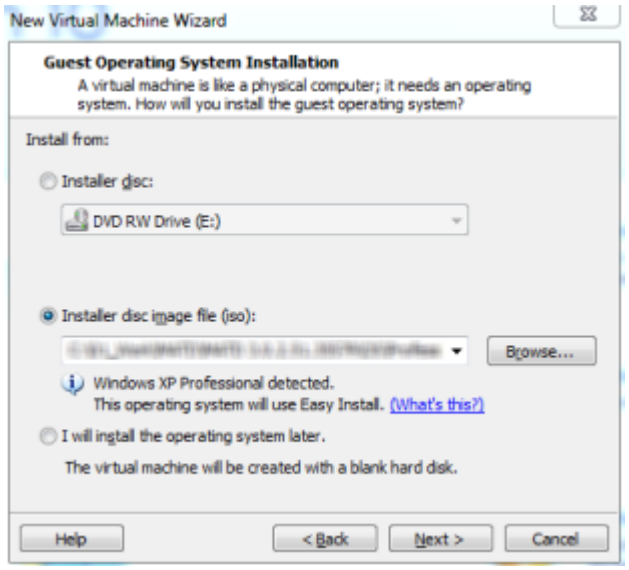
| Step | Details |
|---|---|
| **Step 4:** In the **Choose the Virtual Machine Hardware Compatibility** window, select **Workstation 9.0** from the **Hardware compatibility** drop-down list. For other fields, leave the default values and click **Next**. |  |
| **Step 5:** In the **Guest Operating System Installation** window, select either **Installer disc** or **Installer disc image file (iso)**, browse and select the ISO image, and then click **Next**. |  |

**Table 5-1 Create a VMDK file from Windows XP SP2 or SP3 ISO image.** *(continued)*

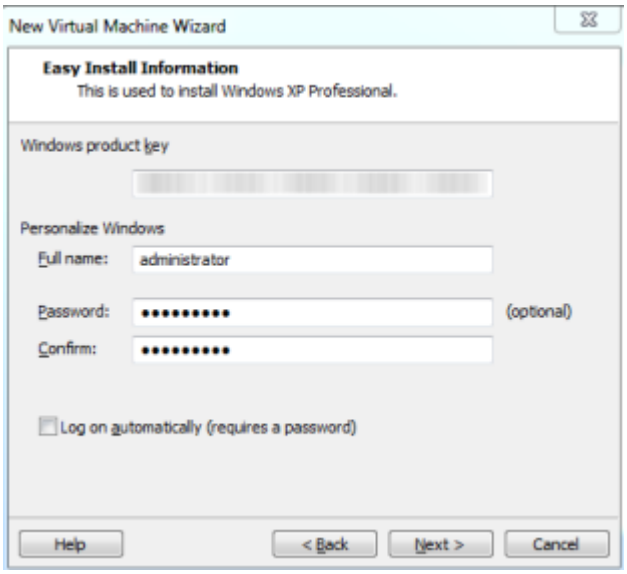
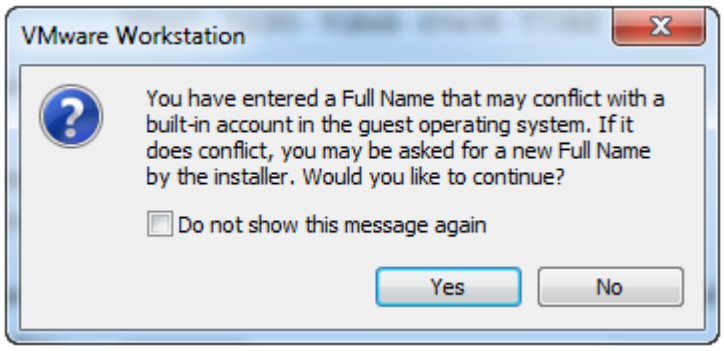
| Step | Details |
|---|---|
| **Step 6:** Enter the information in the **Easy Install Information** window and then click **Next**. | • **Windows product key** — Enter the license key of the Windows operating system for which you are creating the VMDK file.<br>• **Full name** — You must enter `administrator` as the **Full name**.<br>• **Password** — You must enter `cr@cker42` as the password. This is the password that McAfee Advanced Threat Defense uses to log on to the VM.<br>• **Confirm** — Enter `cr@cker42` again to confirm.<br>• **Log on automatically (requires a password)** — Deselect this box.<br>  |
| **Step 7:** If the **VMware Workstation** message displays, click **Yes**. |  |

**Table 5-1 Create a VMDK file from Windows XP SP2 or SP3 ISO image.** *(continued)*

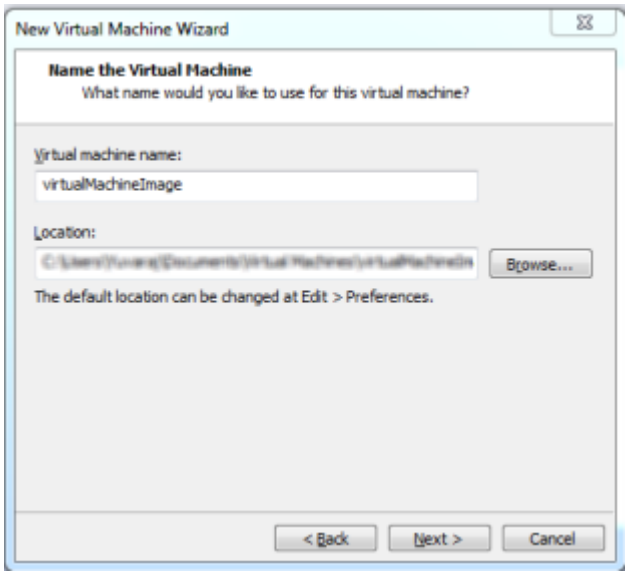
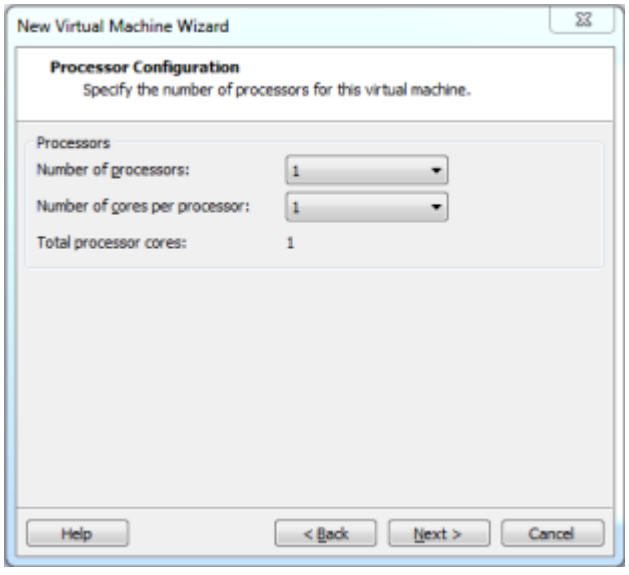
| Step | Details |
|---|---|
| **Step 8:** Enter the information in the **Name the Virtual Machine** window and then click **Next**. | • **Virtual Machine name** — You must enter `virtualMachineImage` as the name.<br>• **Location** — Browse and select the folder where you want to create the VMDK file.<br>  |
| **Step 9:** In the **Processor Configuration** window, leave the default values and click **Next**. |  |

**Table 5-1 Create a VMDK file from Windows XP SP2 or SP3 ISO image.** *(continued)*

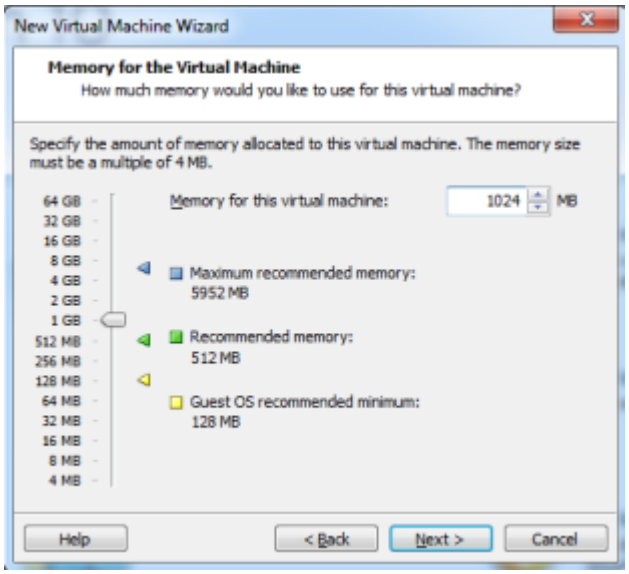
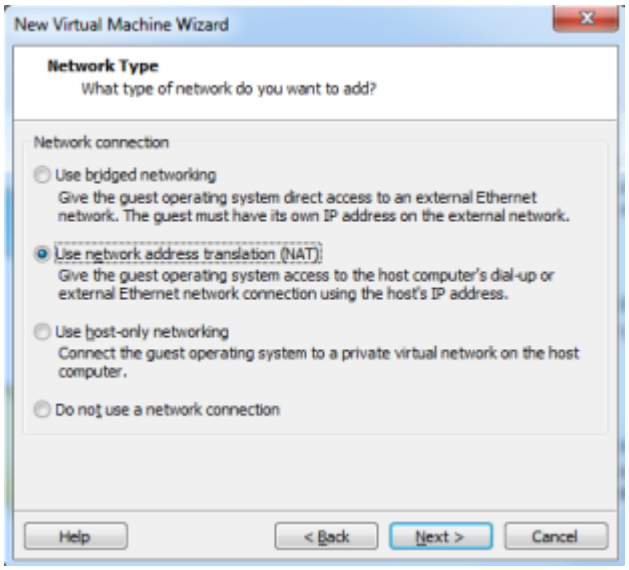
| Step | Details |
|---|---|
| **Step 10:** In the **Memory for the Virtual Machine** window, set 1024 MB as the memory. |  |
| **Step 11:** In the **Network Type** window, leave the default selection. |  |

**Table 5-1 Create a VMDK file from Windows XP SP2 or SP3 ISO image.** *(continued)*

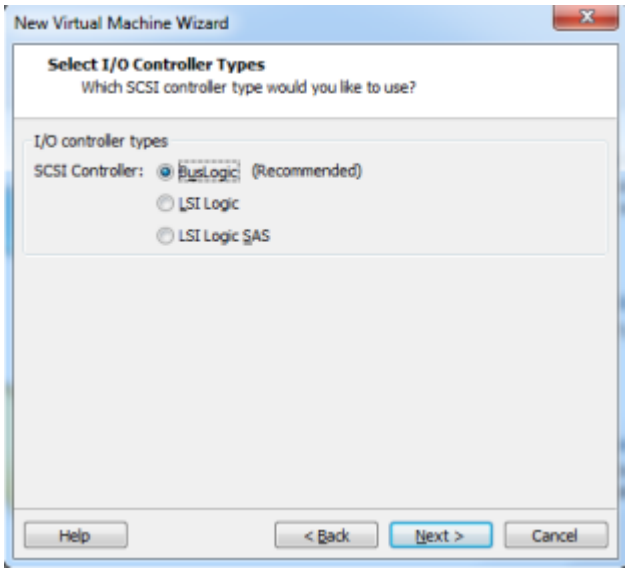
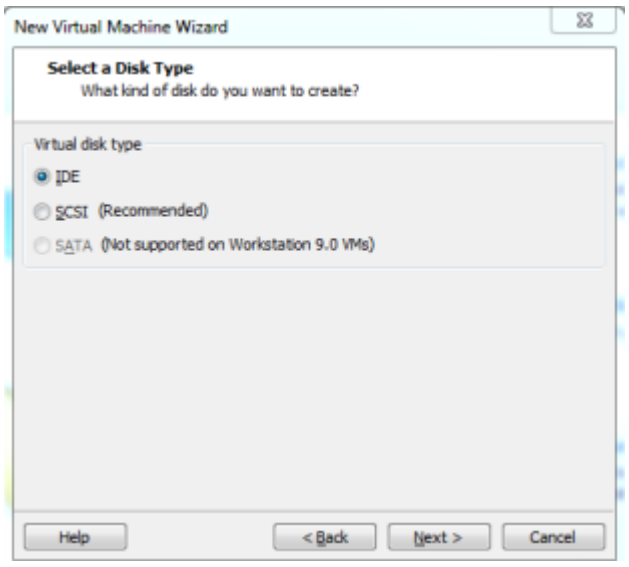
| Step | Details |
|---|---|
| **Step 12:** In the **Select I/O Controller Types** , leave the default selection. |  |
| **Step 13:** In the **Select a Disk Type** page, select **IDE** and click **Next.**<br>SCSI disks are not compatible with McAfee Advanced Threat Defense. |  |

**Table 5-1 Create a VMDK file from Windows XP SP2 or SP3 ISO image.** *(continued)*

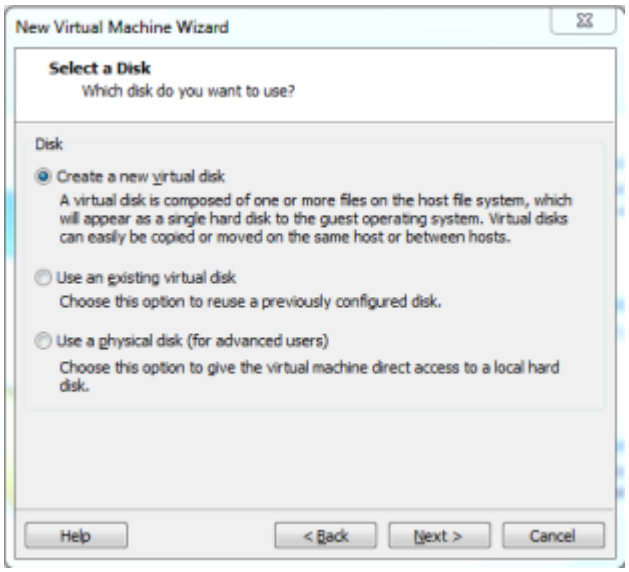
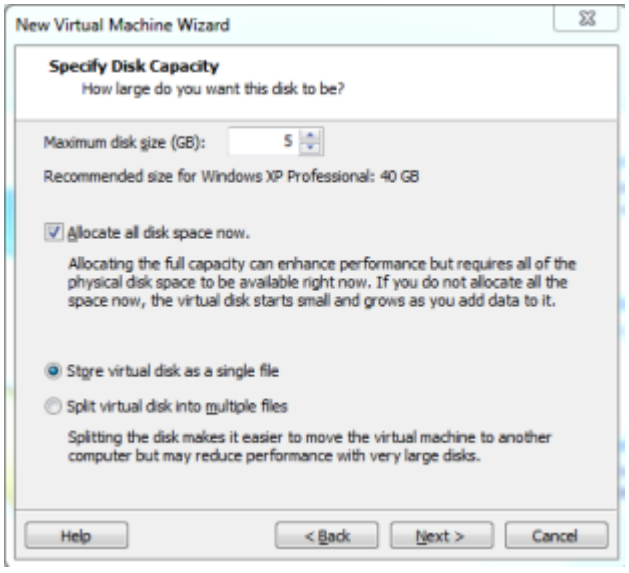
| Step | Details |
|---|---|
| **Step 14:** In the **Select a Disk** window, select **Create a new virtual disk** and click **Next**. |  |
| **Step 15:** Specify the details in the **Specify Disk Capacity** window and then click **Next**. | • **Maximum disk size (GB)** — For Windows XP, the maximum disk size can be 30 GB, however you must enter 5 GB for optimal performance.<br>• Select **Allocate all disk space now.**<br>• Select **Store virtual disk as a single file.**<br>  |

**Table 5-1 Create a VMDK file from Windows XP SP2 or SP3 ISO image.** *(continued)*

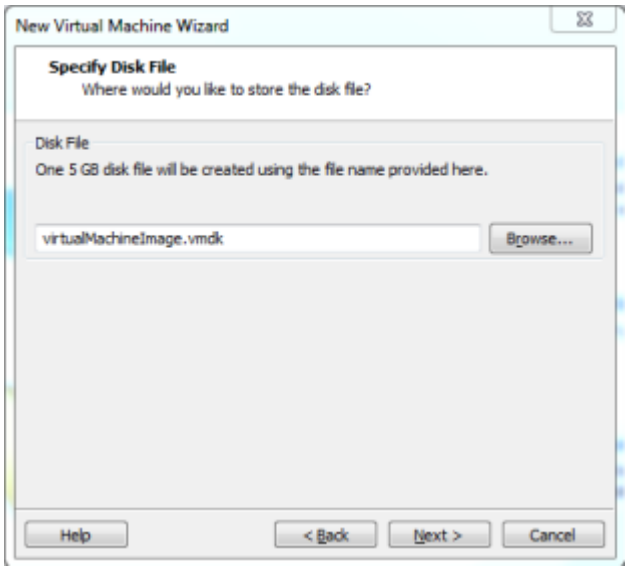
| Step | Details |
|---|---|
| **Step 16:** In the **Specify Disk file** window, make sure virtualMachineImage.vmdk is displayed by default and click **Next.**<br>If you specified a different name for **Virtual Machine name,** that name is displayed here. |  |

**Table 5-1 Create a VMDK file from Windows XP SP2 or SP3 ISO image.** *(continued)*

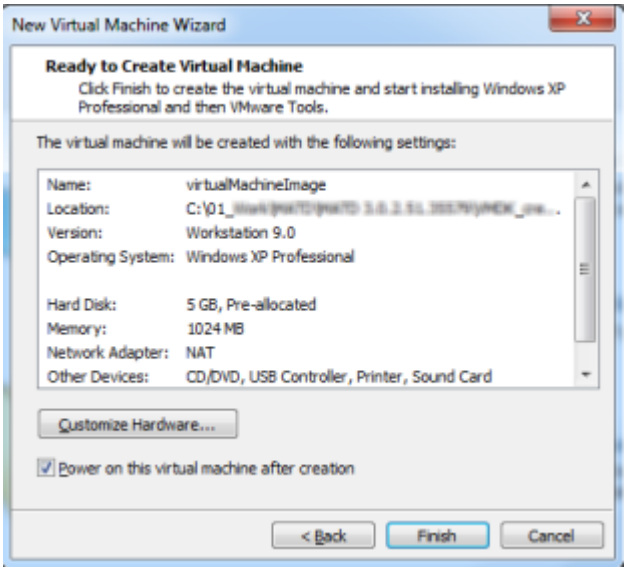
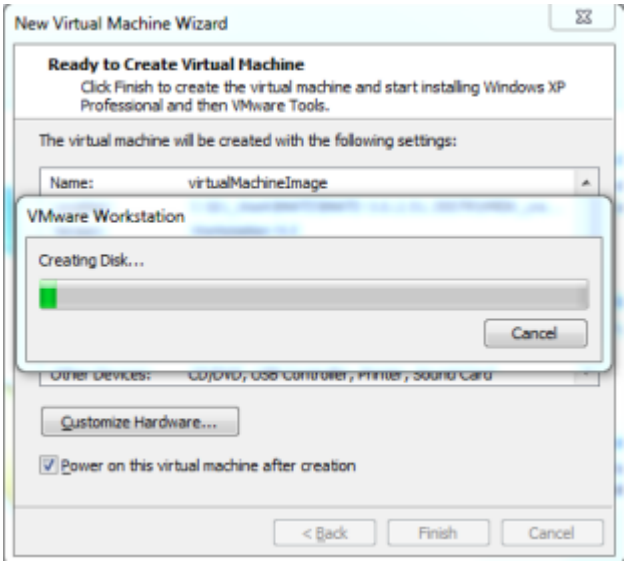
| Step | Details |
|---|---|
| **Step 17:** Complete the following in the **Ready to Create Virtual Machine** window. | • **Power on this virtual machine after creation** — Select this option.<br>• Click **Finish.**<br>This step might take around 30 minutes to complete.<br>  <br><br>  <br> |
| **Step 18:** If the **Removable Devices** pop-up window is displayed, select **Do not show this hint again** and click **OK**. | Windows begins to install, which might take around 15 minutes. |

**Table 5-1 Create a VMDK file from Windows XP SP2 or SP3 ISO image.** *(continued)*

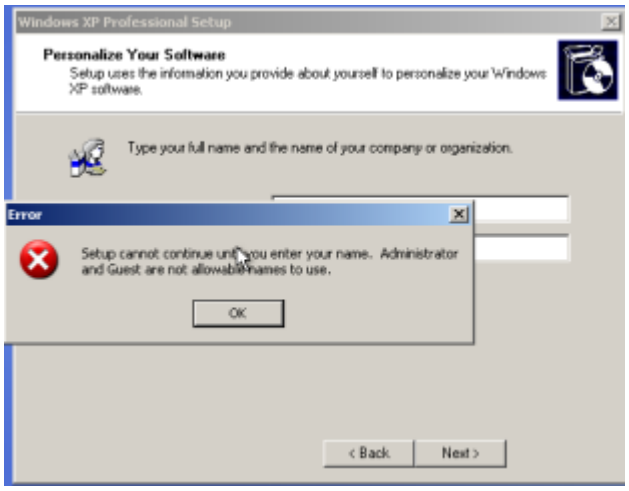
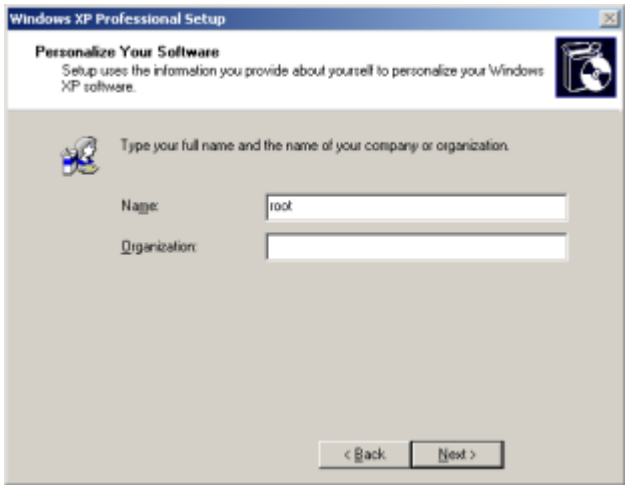
| Step | Details |
|---|---|
| **Step 19:** Click **OK** if the following error message is displayed — *Setup cannot continue until you enter your name. Administrator and Guest are not allowable names to use.* |  |
| **Step 20:** Enter the following details in the **Windows XP Professional Setup** page. | • **Name:** Enter `root`<br>• **Organization:** Leave this blank and click **Next.**<br>This operation might take around 15 minutes.<br>  |
| **Step 21:** Only if prompted, log on to virtualMachineImage with the following credentials. | • **User:** `administrator`<br>• **Password:** `cr@cker42` |

**Table 5-1 Create a VMDK file from Windows XP SP2 or SP3 ISO image.** *(continued)*

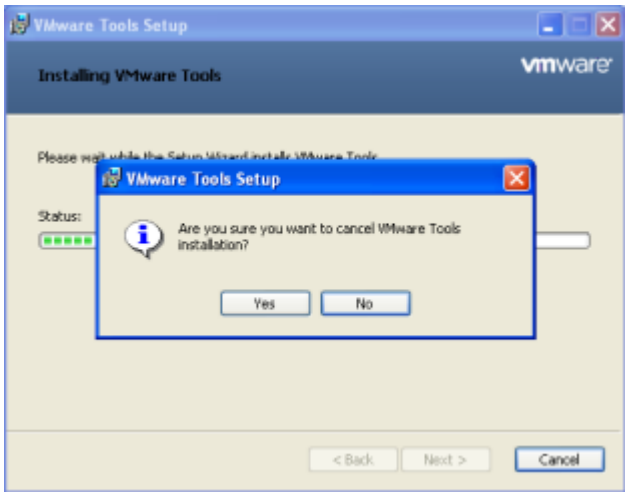
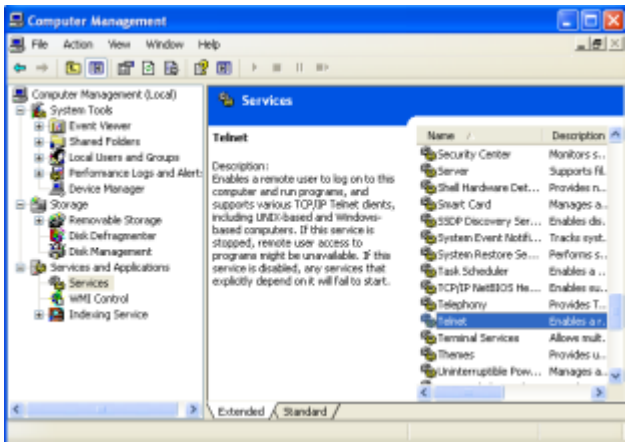
| Step | Details |
|---|---|
| **Step 22:** Stop the VMware Tools installation.<br>The VMware Tools are not compatible with McAfee Advanced Threat Defense. If you did not stop the VMware Tools installation, you can continue with the VMDK file creation process but make sure it is uninstalled when the VMDK file is ready. |  |
| **Step 23:** In the virtualMachineImage, select **Start** \| **Control Panel** \| **Security Center** \| **Windows Firewall** \| **OFF.** | |
| **Step 24:** In the virtualMachineImage VM, click **Start** and right-click **My Computer**. Then select **Manage** \| **Services and Applications** \| **Services.** Then double-click **Telnet.** |  |

**Table 5-1 Create a VMDK file from Windows XP SP2 or SP3 ISO image.** *(continued)*

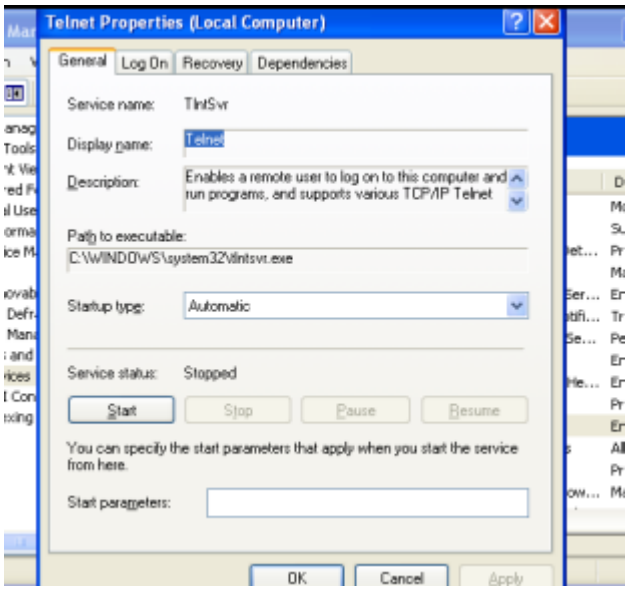
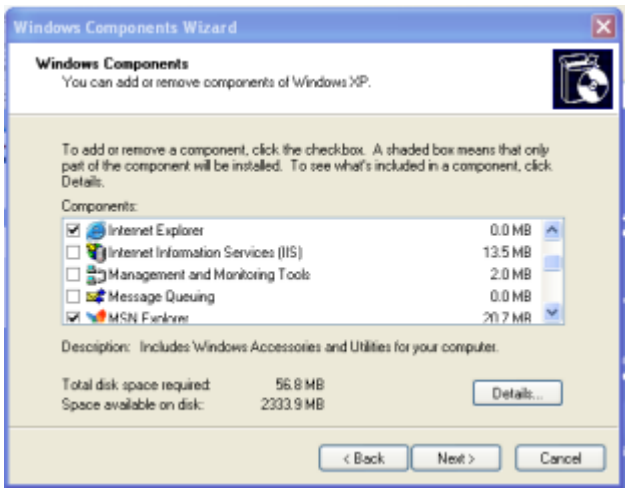
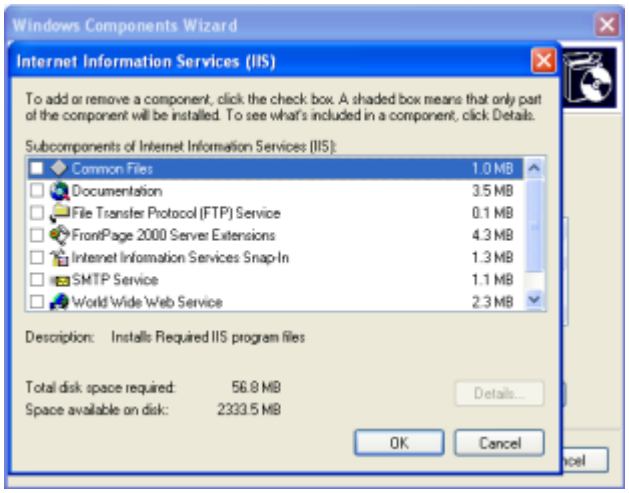
| Step | Details |
|---|---|
| **Step 25:** In the **Telnet Properties(Local Computer)** window, you must select **Automatic** from the **Startup type** drop-down list. Then select **Apply** \| **Start** \| **OK**. |  |
| **Step 26:** Enable FTP on the VM.<br>In the virtualMachineImage, select **Start** \| **Control Panel** \| **Add or remove Programs** \| **Add or remove Windows components.**. |  |
| **Step 27:** In the **Windows Components** wizard, double-click **Internet Information Services(IIS)**. |  |

**Table 5-1 Create a VMDK file from Windows XP SP2 or SP3 ISO image.** *(continued)*

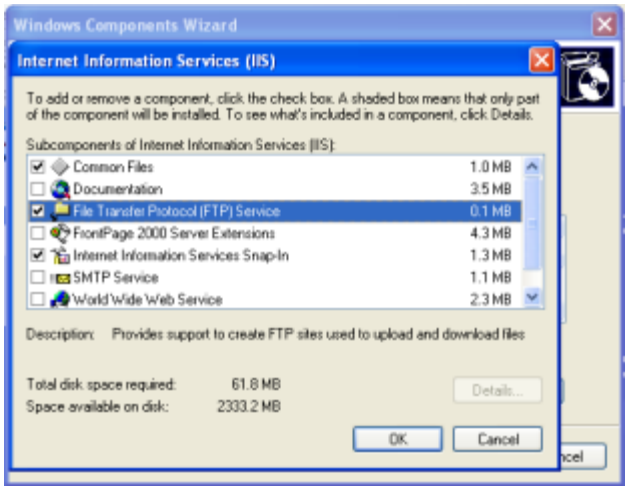
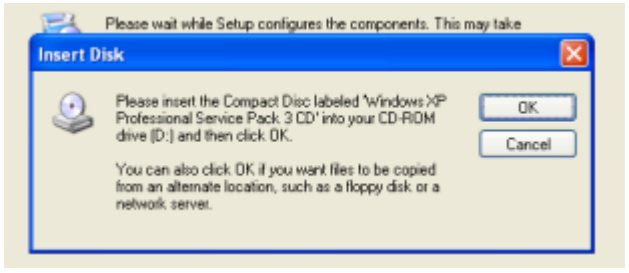
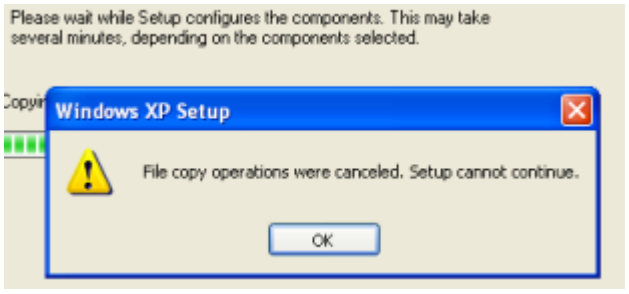
| Step | Details |
|---|---|
| **Step 28:** In the **Internet Information Services(IIS)** pop-up window, complete the following. | 1 Select **File Transfer Protocol (FTP) Service**.<br>2 Select **Common Files**.<br>3 Select **Internet Information Services Snap-In**, click **OK**, and then click **Next**.<br>  |
| **Step 29:** In the **Insert Disk** pop-up, click **Cancel**. |  |
| **Step 30:** In the **Windows XP Setup** pop-up, select **OK**. |  |

**Table 5-1 Create a VMDK file from Windows XP SP2 or SP3 ISO image.** *(continued)*

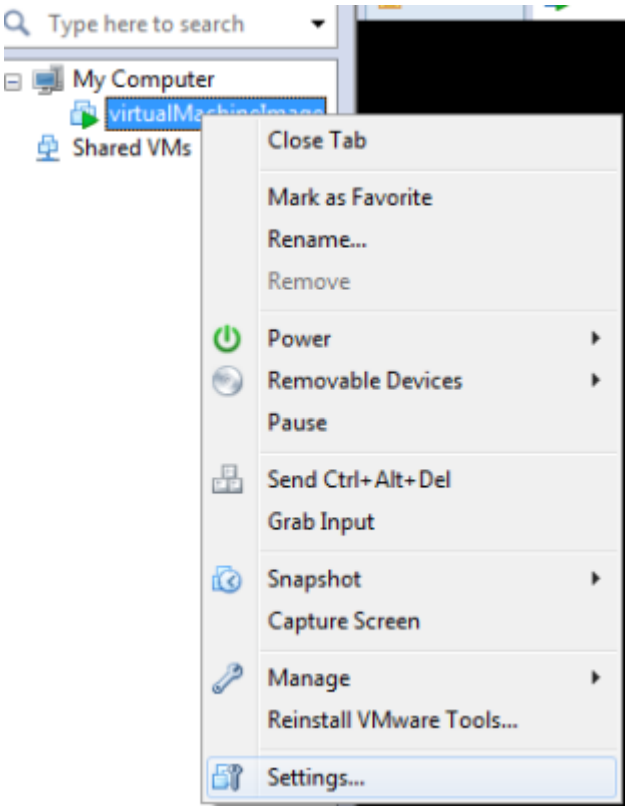
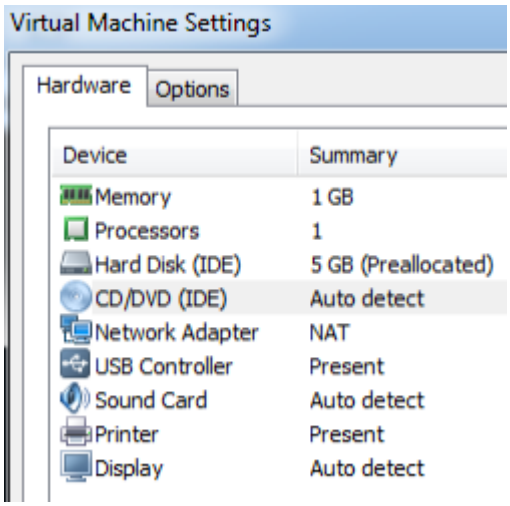
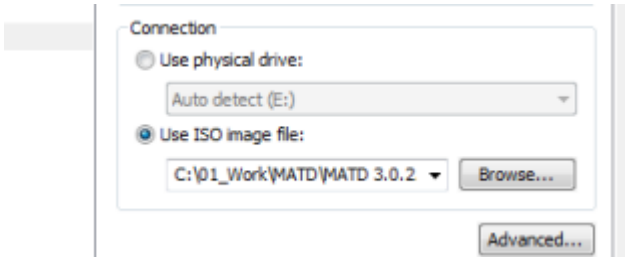
| Step | Details |
|---|---|
| **Step 31:** In the VMware Workstation, right-click on the VM, which in this example is virtualMachineImage. Then select **Settings**. |  |
| **Step 32:** In the Virtual Machine Settings window, select **CD/DVD (IDE)**. |  |
| **Step 33:** In the **Use ISO image file** field, browse to the ISO file that you used and press **OK**. |  |

**Table 5-1 Create a VMDK file from Windows XP SP2 or SP3 ISO image.** *(continued)*

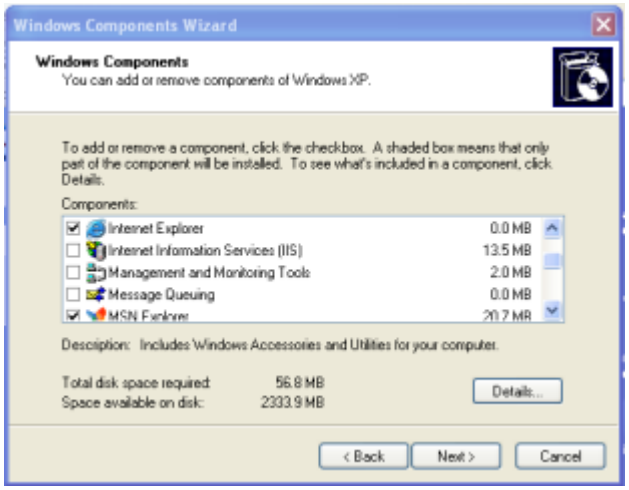
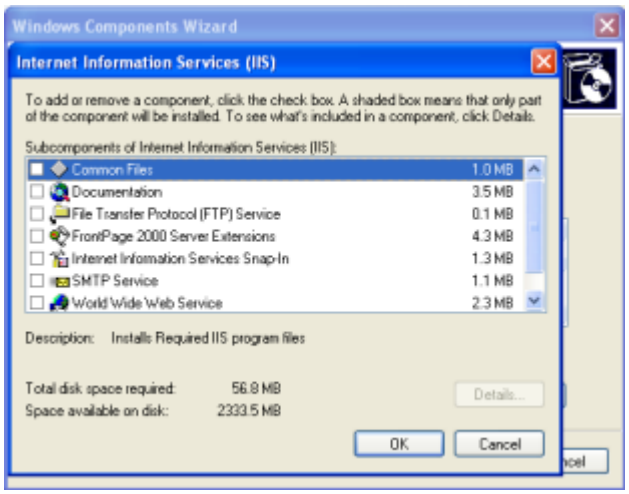
| Step | Details |
|---|---|
| **Step 34:** In the **Welcome to Microsoft Windows XP** page, click **Exit.** | |
| **Step 35:** In the virtualMachineImage, select **Start \| Control Panel \| Add or remove Programs \| Add or remove Windows components..** |  |
| **Step 36:** In the **Windows Components** wizard, double-click **Internet Information Services(IIS).** |  |

**Table 5-1 Create a VMDK file from Windows XP SP2 or SP3 ISO image.** *(continued)*

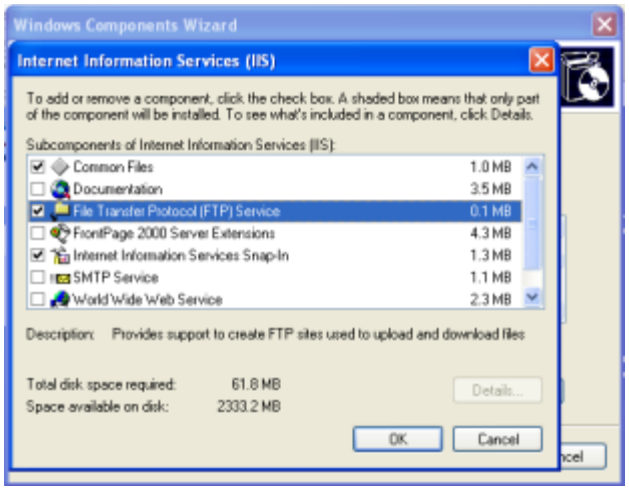
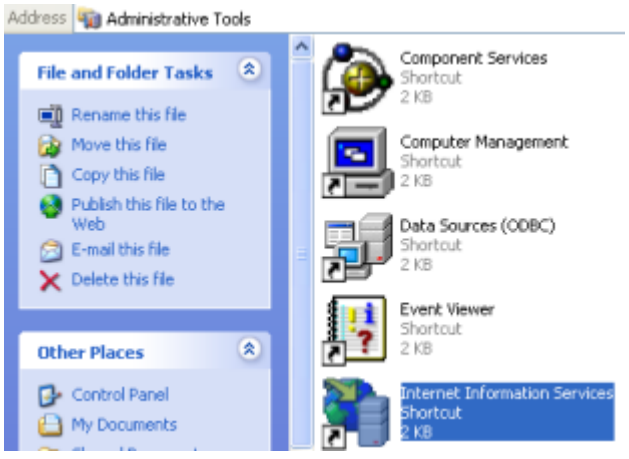
| Step | Details |
|---|---|
| **Step 37:** In the **Internet Information Services(IIS)** pop-up window, complete the following. | 1 Select **File Transfer Protocol (FTP) Service**.<br>2 Select **Common Files**.<br>3 Select **Internet Information Services Snap-In**, click **OK**, and then click **Next**.<br>  |
| **Step 38:** In the **Windows Components Wizard**, click **Finish** to finish installing FTP. | |
| **Step 39:** Select **Start** \| **Control Panel** \| **Switch to Classic View** \| **Administrative Tools** and double-click **Internet Information Services**. |  |

**Table 5-1 Create a VMDK file from Windows XP SP2 or SP3 ISO image.** *(continued)*

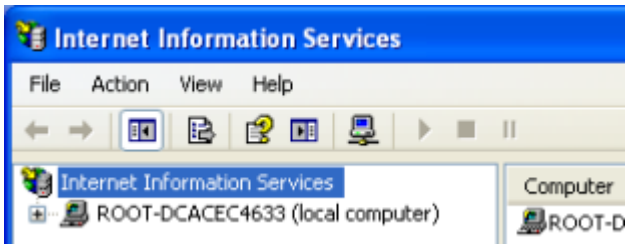
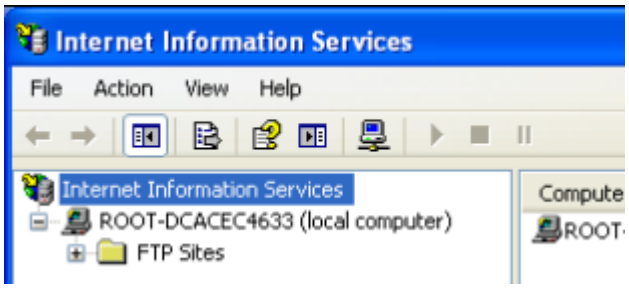
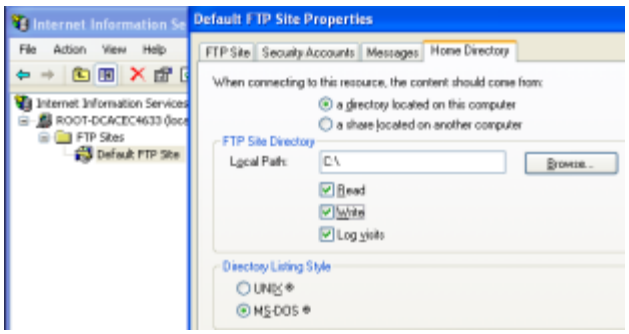
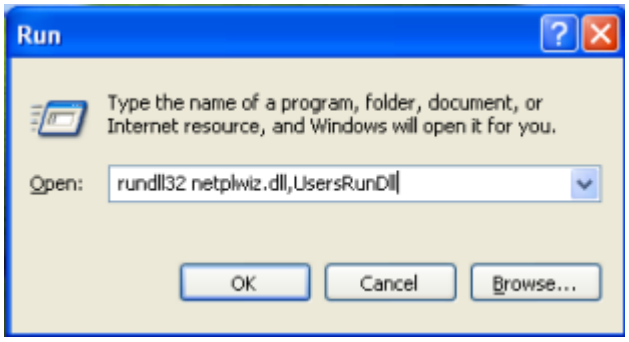
| Step | Details |
|---|---|
| **Step 40:** In the **Internet Information Services** widnow, expand + below **Internet Information Services.** |  |
| **Step 41:** Expand **FTP Sites.** |  |
| **Step 42:** Right-click on **Default FTP Site** and then select **Properties** \| **Home Directory** . Then complete the following.<br>1 Browse to C:\<br>2 Select **Read.**<br>3 Select **Write.**<br>4 Select **Log visits** and click **Apply** and then **OK.** |  |
| **Step 43:** Set automatic logon by selecting **Start** \| **Run**, enter `rundll32 netplwiz.dll,UsersRunDll` and press **Enter**. |  |

**Table 5-1 Create a VMDK file from Windows XP SP2 or SP3 ISO image.** *(continued)*

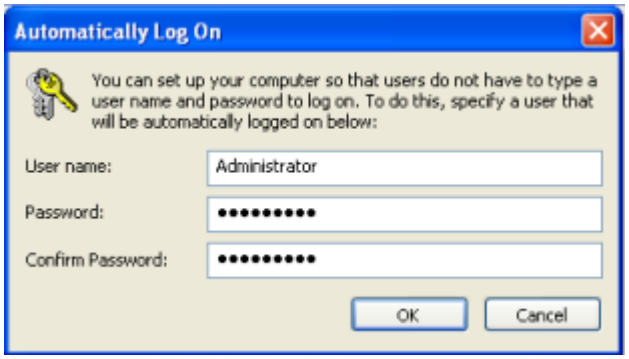
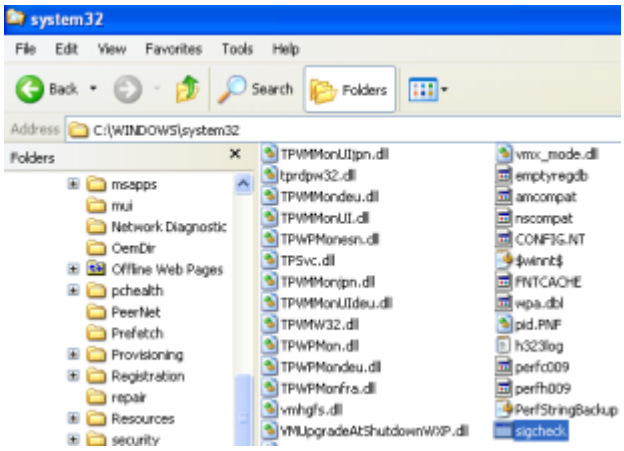
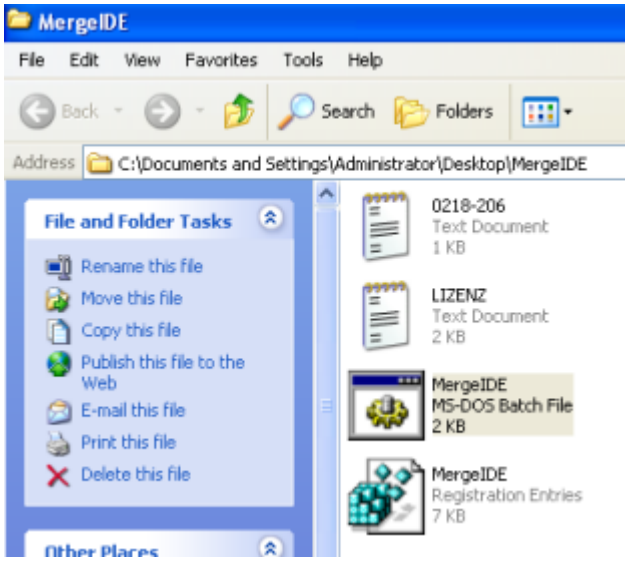
| Step | Details |
|---|---|
| **Step 44:** In the **User Accounts** window, deselect **Users must enter a user name and password to use this computer** and click **Apply**. | |
| **Step 45:** In the **Automatically Log On** pop-up window, complete the following and then press **OK** in the message boxes. | • **User name** — Enter `Administrator`<br>• **Password** — Enter `cr@cker42`<br>• **Confirm Password** — Enter `cr@cker42`<br>  |
| **Step 46:** Download Sigcheck on to your computer (the native host) from http://technet.microsoft.com/en-us/sysinternals/bb897441.aspx. | The VM that you created has the Windows Firewall switch off as well as there is no anti-virus installed on it. Therefore, it is recommended that you download the programs and components on to the native host first and then copy them to the VM in VMware Workstation. |

**Table 5-1 Create a VMDK file from Windows XP SP2 or SP3 ISO image.** *(continued)*

| Step | Details |
|---|---|
| **Step 47:** Extract sigcheck.zip to `C:\WINDOWS\system32` location. |  |
| **Step 48:** In Windows Explorer, go to C:\ WINDOWS \system32 and double-click **sigcheck.exe**. | |
| **Step 49:** If prompted, click **Run** in the warning message. | |
| **Step 50:** Click **Agree** for **Sigcheck License Agreement.**<br><br>After you click on **Agree**, no confirmation message is displayed. | |
| **Step 51:** Download MergeIDE.zip from https://www.virtualbox.org/attachment/wiki/Migrate_Windows/MergeIDE.zip on to the native computer and then copy it to the VM. |  |



SigCheck License Agreement
You can also use the /accepteula command-line switch to accept the EULA.
SYSINTERNALS SOFTWARE LICENSE TERMS
These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Systinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals
updates,
supplements,
Internet-based services, and
Print
Agree
Decline

**Table 5-1 Create a VMDK file from Windows XP SP2 or SP3 ISO image.** *(continued)*

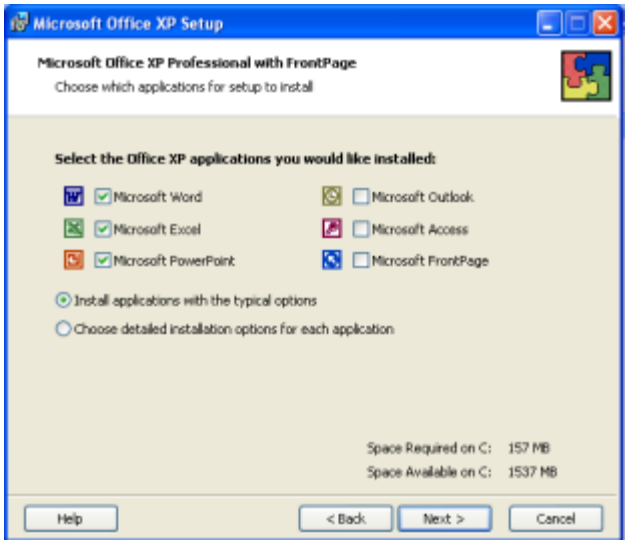
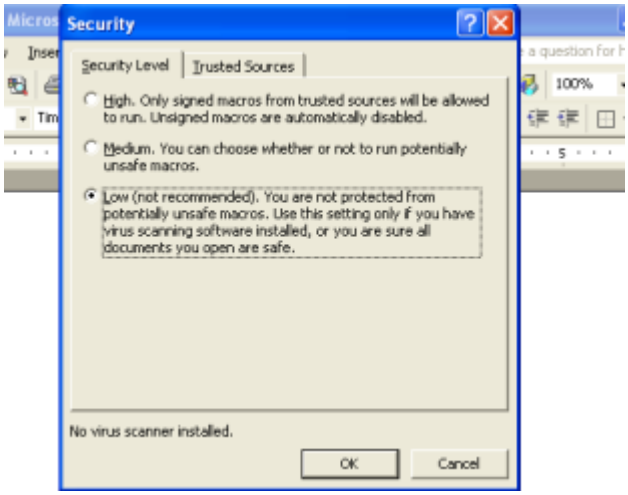
| Step | Details |
|---|---|
| **Step 52:** Extract MergeIDE.zip and run the MergeIDE batch file in the VM. | • If prompted, select **Run** in the warning message.<br>• Close Windows Explorer. |
| **Step 53:** Disable Windows updates. | 1 Select **Start** \| **Settings** \| **Control Panel**.<br>2 Open **System**.<br>3 In the **Automatic Updates** tab, deselect **Keep my computer up to date.**<br>4 Click **Apply** and then **OK**. |
| **Step 54:** To analyze Microsoft Word, Excel, and Powerpoint files, install Microsoft Office 2003 on the virtual machine. |  |
| **Step 55:** Lower the security to run macros for the Office applications. | • Open Microsoft Word 2003 and select **Tools** \| **Macro** \| **Security** and then select **Low** and click **OK**.<br>  <br>• Similarly lower the macro security for Microsoft Excel and Powerpoint. |

**Table 5-1 Create a VMDK file from Windows XP SP2 or SP3 ISO image.** *(continued)*

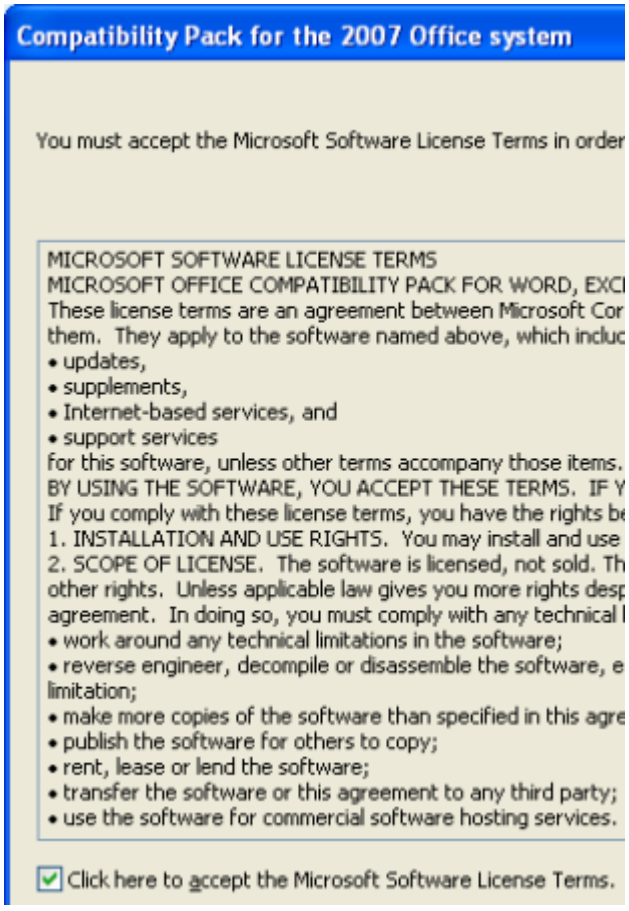
| Step | Details |
|---|---|
| **Step 56:** You need the compatibility pack to open Microsoft Office files that were created in a newer version of Microsoft Office. For example, to open a .docx file using Office 2003, you need the corresponding compatibility pack installed.<br>Go to http://www.microsoft.com/en-us/download/details.aspx?id=3 and download the required Microsoft Office compatibility pack for Word, Excel, and PowerPoint File Formats. Then install them on the virtual machine. | |
| **Step 57:** In the **Compatibility Pack for the 2007 Office system** dialog, select **Click here to accept the Microsoft Software License Terms** and click **OK**. |  |

**Table 5-1 Create a VMDK file from Windows XP SP2 or SP3 ISO image.** *(continued)*

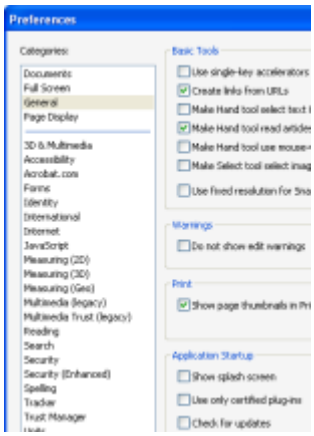
| Step | Details |
|---|---|
| **Step 58:** To analyze PDF files, download Adobe Reader to the native host and copy it to the VM.<br><br>This procedure uses Adobe Reader 9.0 as an example. | 1 Install Adobe Reader 9.0 in the VM.<br>2 Open Adobe Reader and click **Accept**.<br> <br>3 In Adobe Reader, select **Edit** \| **Preferences** \| **General** and deselect **Check for updates**.<br>  |
| **Step 59:** Download the following on to the native host and then install them on the VM. | 1 Download Microsoft Visual C++ 2005 Redistributable Package (x86) from http://www.microsoft.com/en-us/download/details.aspx?id=3387and install it.<br>2 Download Microsoft Visual C++ 2008 Redistributable Package (x86) from http://www.microsoft.com/en-us/download/details.aspx?id=5582and install it.<br>3 Download Microsoft Visual C++ 2010 Redistributable Package (x86) from http://www.microsoft.com/en-us/download/details.aspx?id=5555and install it.<br>4 Download Microsoft .NET Framework 2.0 Service Pack 2 (x86 version) from http://www.microsoft.com/en-us/download/details.aspx?id=1639and install it. |

**Table 5-1 Create a VMDK file from Windows XP SP2 or SP3 ISO image.** *(continued)*

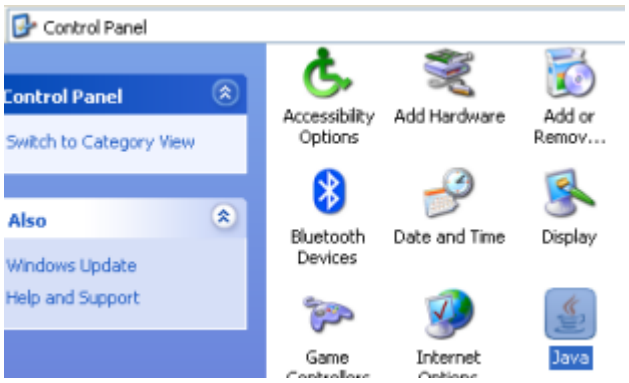
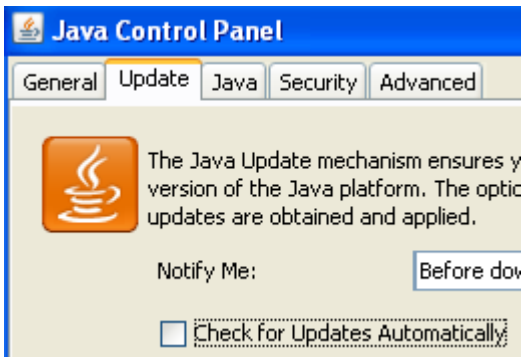
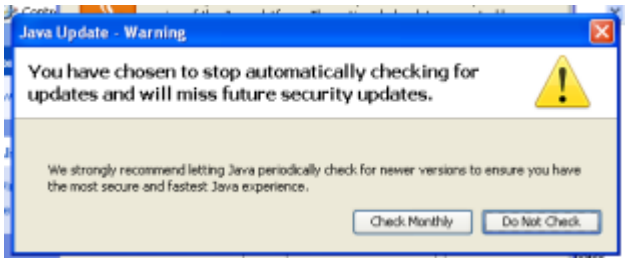
| Step | Details |
|---|---|
| **Step 60:** To analyze JAR files, download and install Java Runtime Environment.<br><br>This procedure uses Java 7 Update 25 as an example. | |
| **Step 61:** Open Java in the Control Panel. |  |
| **Step 62:** In the **Update** tab, deselect **Check for Updates Automatically.** |  |
| **Step 63:** In the Java Update Warning dialog, select **Do Not Check** and then click **OK** in the Java Control Panel. |  |

**Table 5-1 Create a VMDK file from Windows XP SP2 or SP3 ISO image.** *(continued)*

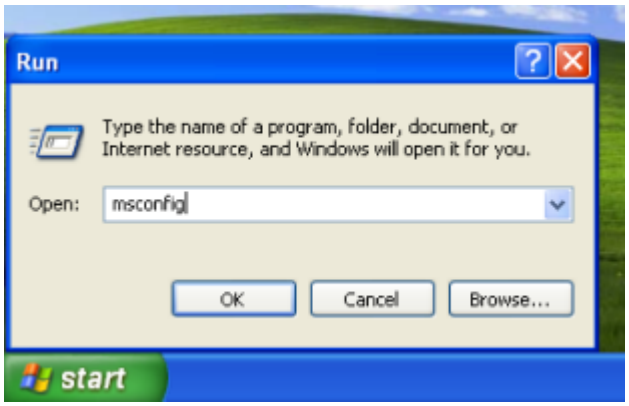
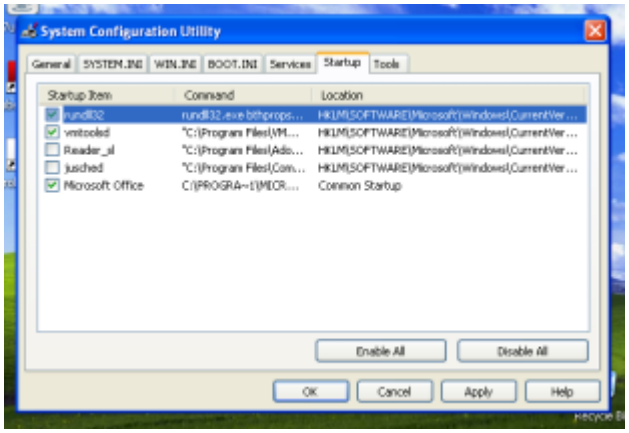
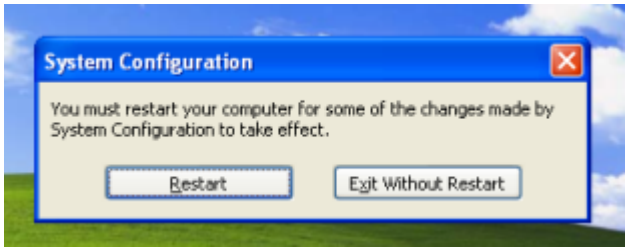
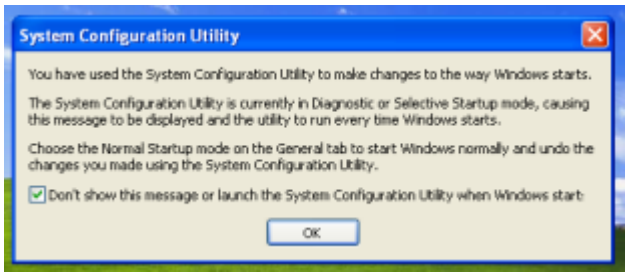
| Step | Details |
|---|---|
| **Step 64:** In the Windows Run dialog, enter `msconfig`. |  |
| **Step 65:** In the System Configuration utility, go to the **Startup** tab. |  <br>Deselect *reader_sl* and *jusched* and then click **OK**. |
| **Step 66:** In the **System Configuration** dialog, click **Restart**. |  |
| **Step 67:** In the **System Configuration Utility** dialog, select **Don't show this message or launch the System Configuration Utility when Windows start** and click **OK**. |  |

**Table 5-1 Create a VMDK file from Windows XP SP2 or SP3 ISO image.** *(continued)*

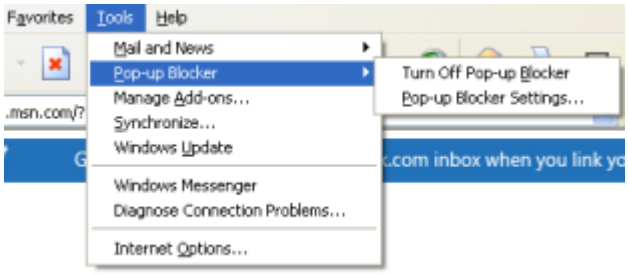
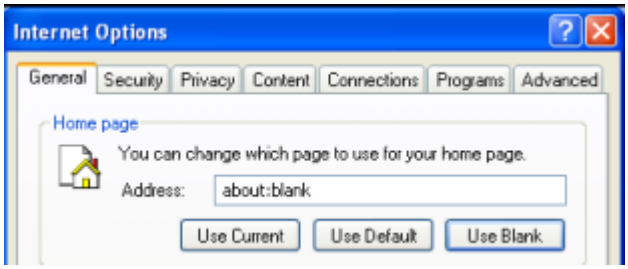
| Step | Details |
|---|---|
| **Step 68:** Open the default browser and set it up for malware analysis.<br><br>This procedure uses Internet Explorer as an example. | 1 Make sure the pop-up blocker is turned on. In Internet Explorer, select **Tools** \| **Pop-up Blocker** \| **Turn on Pop-up Blocker.**<br><br>  <br><br>2 Select **Tools** \| **Internet Options** and for **Home page** select **Use Blank** or **Use new tab** based on the version of Internet Explorer.<br><br>  <br><br>3 Go to the **Advanced** tab of the Internet Options and locate **Security.**<br><br>4 Select **Allow active content to run in files on My Computer.** |

**Table 5-1 Create a VMDK file from Windows XP SP2 or SP3 ISO image.** *(continued)*

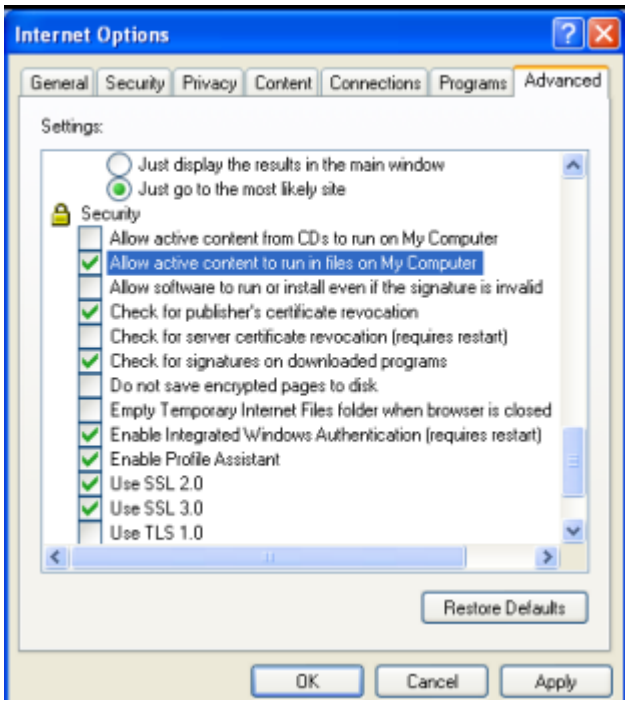
| Step | Details |
|---|---|
| |  <br>**5** Click **OK**. |

**Table 5-1 Create a VMDK file from Windows XP SP2 or SP3 ISO image.** *(continued)*

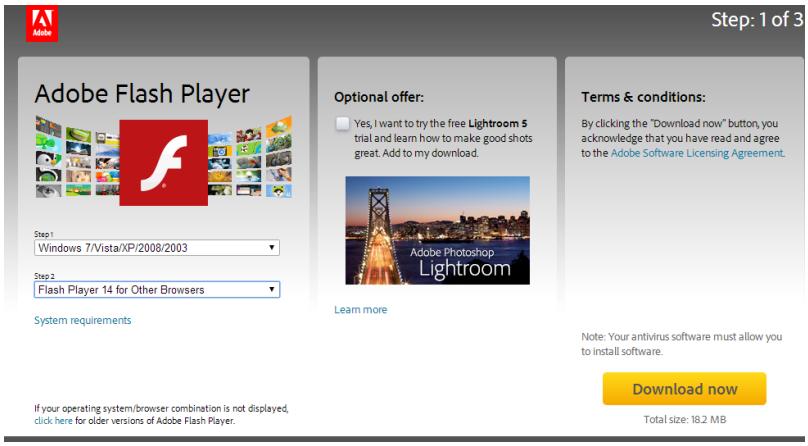
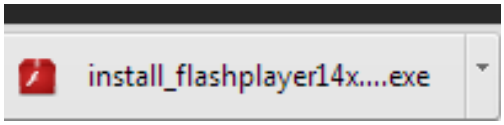
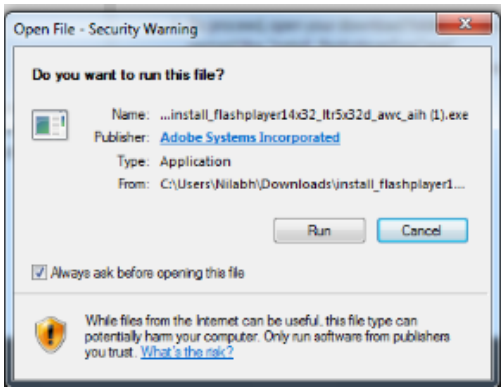
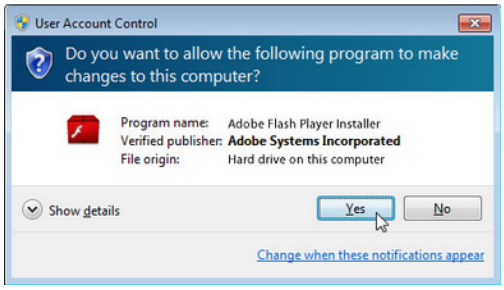
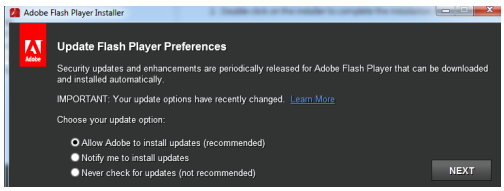
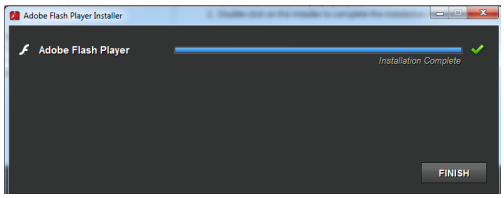
| Step | Details |
|---|---|
| **Step 69:** To dynamically analyze Flash files (SWF), install the required version of Adobe Flash.<br><br>This procedure uses Flash Player 14 as an example. | 1 Goto http://get.adobe.com/flashplayer/otherversions/.<br><br>2 Select Operating System and Flash Player version respectively as per your requirement in **Step 1** and **Step 2** drop-down as shown below.<br><br>3 Click on **Download now** tab.<br><br>  <br><br>4 Double-click the Adobe Flash Player Installer file **(install_flashplayer xxx.exe)**, present at the bottom corner of your screen.<br><br>  <br><br>5 In the**Security Warning dialogue box**, Click **Run**.<br><br>  <br><br>6 In the **User Account Control** dialogue box, Click **Yes**. |

**Table 5-1 Create a VMDK file from Windows XP SP2 or SP3 ISO image.** *(continued)*

| Step | Details |
|---|---|
| |  <br>7 Choose your update option and Click **NEXT**.<br>  <br>8 Click **FINISH** to complete Adobe Flash Player installation.<br>  |
| **Step 70:** Shut down virtualMachineImage by selecting **Start** \| **Shut down.** | |
| **Step 71:** Go to the location that you provided in step 8 to find the VMDK file named as `virtualMachineImage-flat.vmdk` | |

# Create a VMDK file for Windows 2003 Server

**Before you begin**

- Download VMware Workstation 9.0 or above from http://www.vmware.com/products/workstation/workstation-evaluation and install it.
- Make sure you have the ISO image of the operating system whose VMDK file you need to create.
- Make sure you have the license key for the operating system.

**Table 5-2 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image**

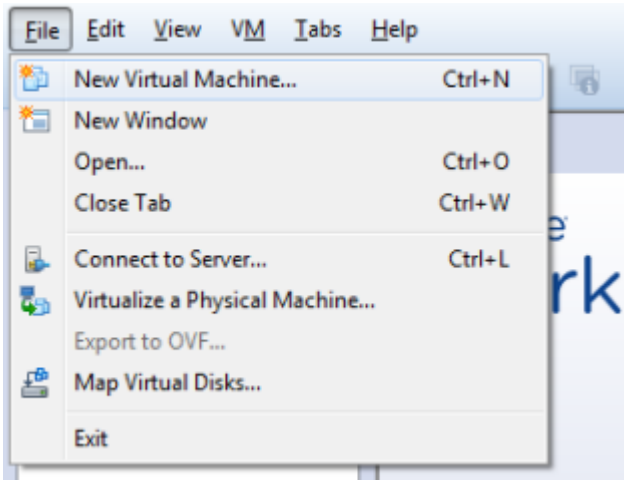
| Step | Details |
|---|---|
| **Step 1:** Start the VMware Workstation. | This procedure uses VMware Workstation 10 as an example. |
| **Step 2:** In the VMware Workstation page, select **File** \| **New Virtual Machine**. |  |
| **Step 3:** In the **New Virtual Machine Wizard** window, select **Custom (Advanced)** and click **Next**. | |

**Table 5-2 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image** *(continued)*

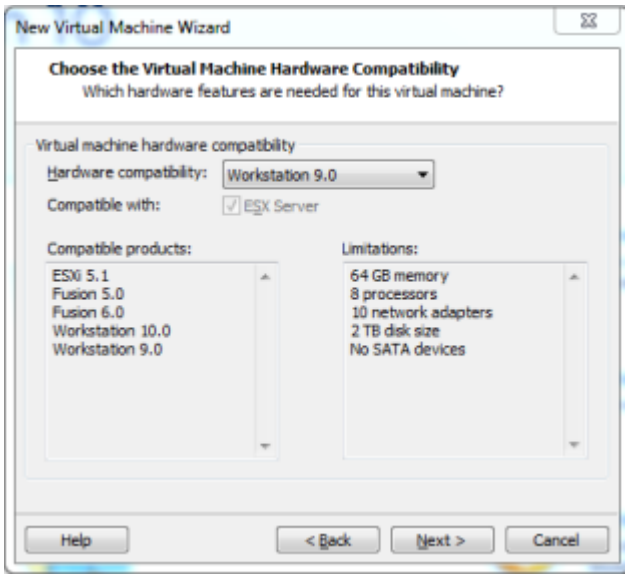
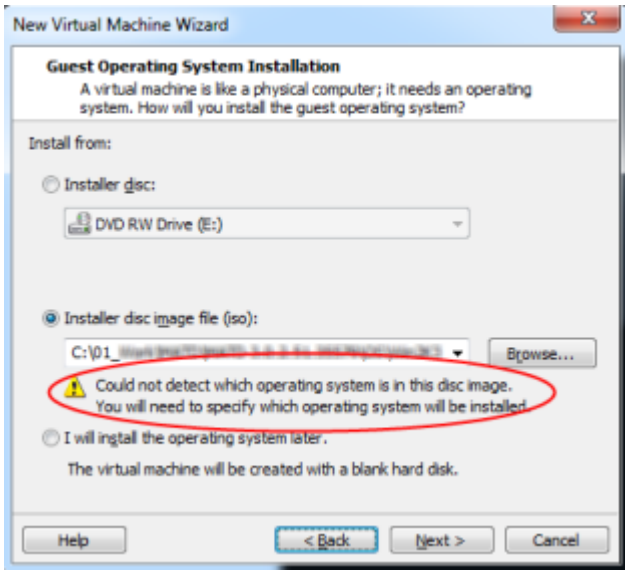
| Step | Details |
|---|---|
| **Step 4:** In the **Choose the Virtual Machine Hardware Compatibility** window, select **Workstation 9.0** from the **Hardware compatibility** drop-down list. For other fields, leave the default values and click **Next**. |  |
| **Step 5:** In the **Guest Operating System Installation** window, select either **Installer disc** or **Installer disc image file (iso)**, browse and select the ISO image, and then click **Next**. |  |

**Table 5-2 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image** *(continued)*

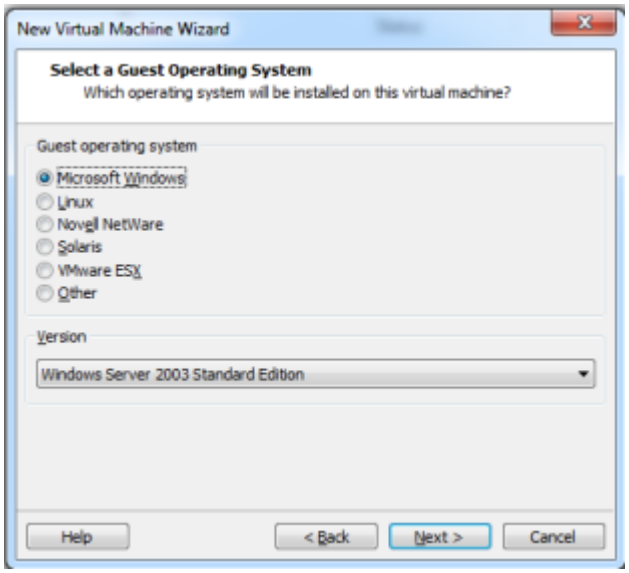
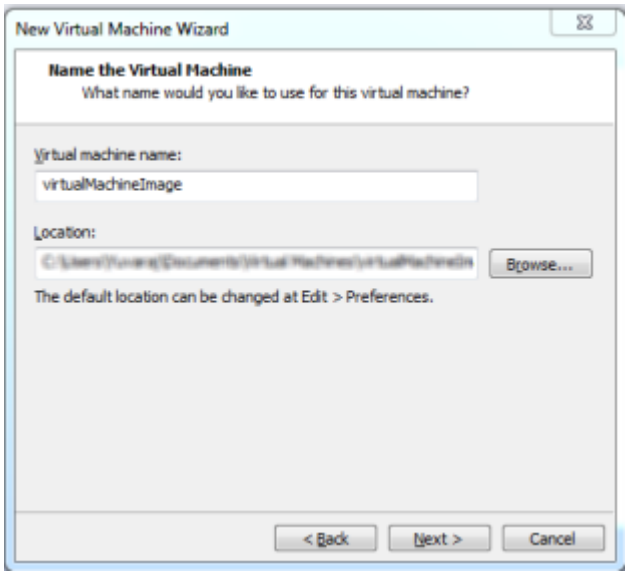
| Step | Details |
|---|---|
| **Step 6:** In the **Select a Guest Operating System** window, select the corresponding version. |  |
| **Step 7:** Enter the information in the **Name the Virtual Machine** window and then click **Next**. | • **Virtual Machine name** — You must enter `virtualMachineImage` as the name.<br>• **Location** — Browse and select the folder where you want to create the VMDK file.<br>  |

**Table 5-2 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image** *(continued)*

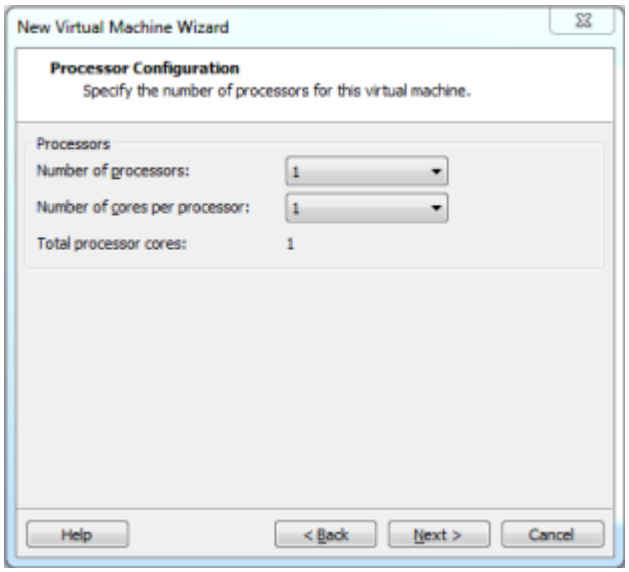
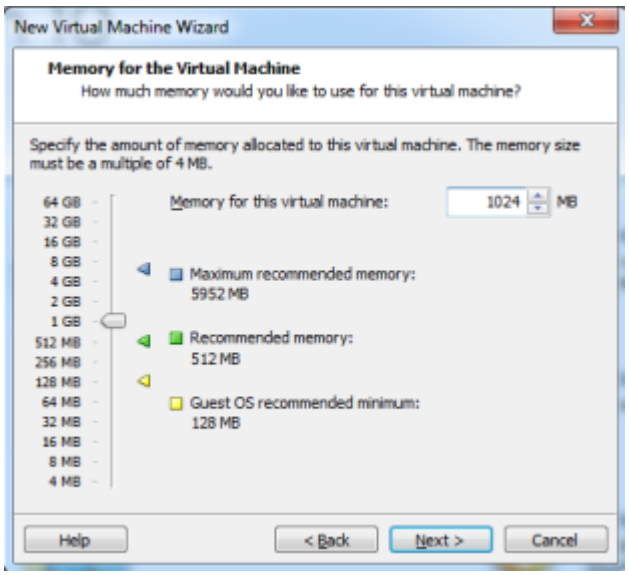
| Step | Details |
|---|---|
| **Step 8:** In the **Processor Configuration** window, leave the default values and click **Next**. |  |
| **Step 9:** In the **Memory for the Virtual Machine** window, set 1024 MB as the memory. |  |

**Table 5-2 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image** *(continued)*

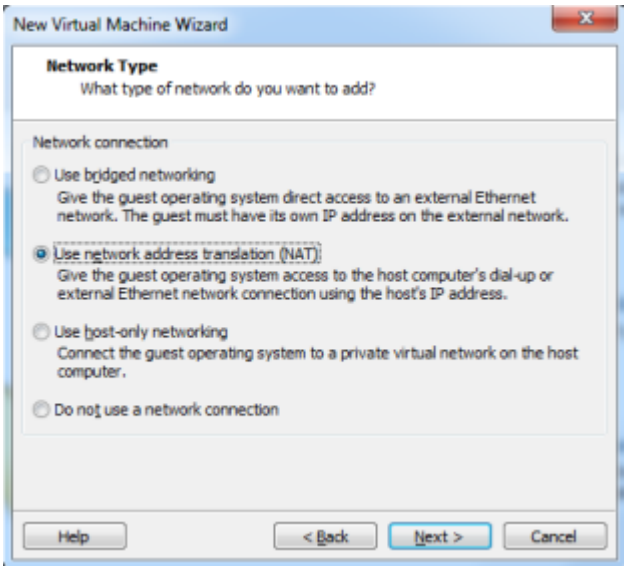
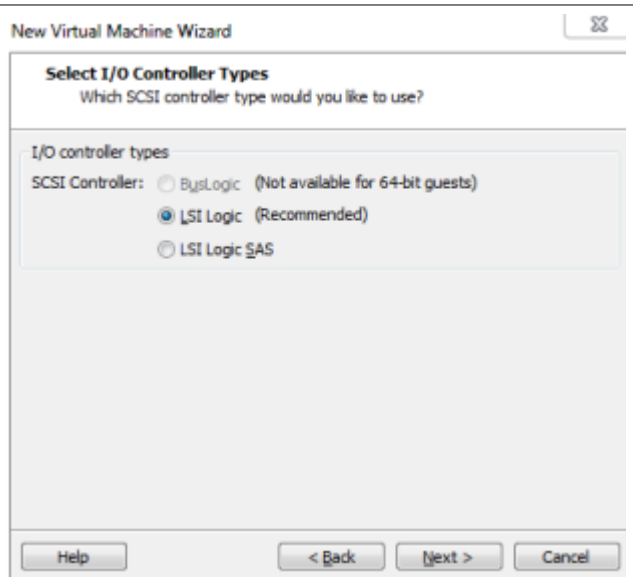
| Step | Details |
|---|---|
| **Step 10:** In the **Network Type** window, leave the default selection. |  |
| **Step 11:** In the **Select I/O Controller Types** , leave the default selection. |  |

**Table 5-2 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image** *(continued)*

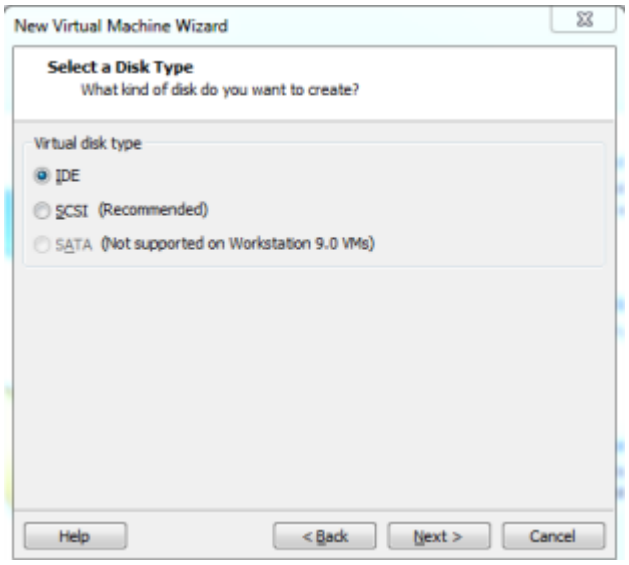
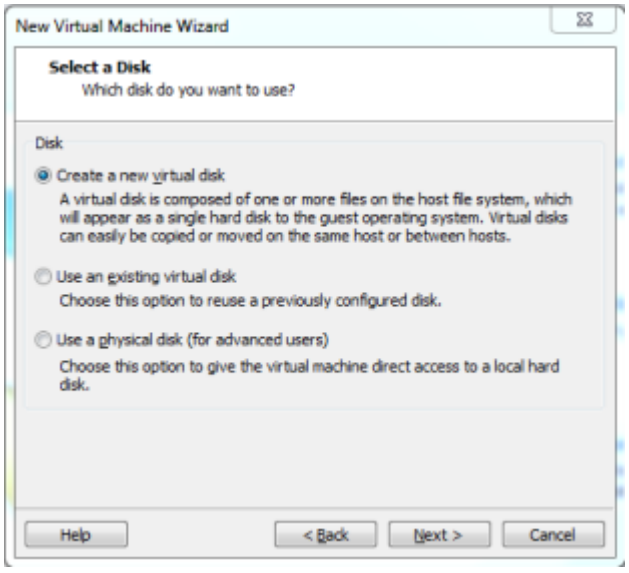
| Step | Details |
|---|---|
| **Step 12:** In the **Select a Disk Type** page, select **IDE** and click **Next**.<br><br>SCSI disks are not compatible with McAfee Advanced Threat Defense. |  |
| **Step 13:** In the **Select a Disk** window, select **Create a new virtual disk** and click **Next**. |  |

**Table 5-2 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image** *(continued)*

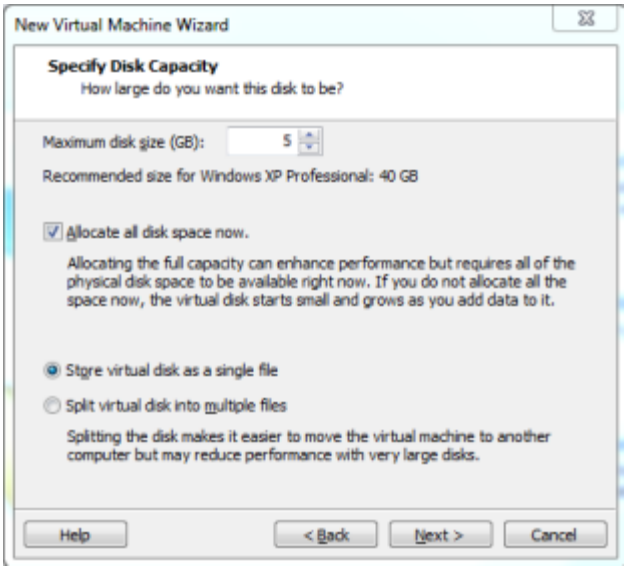
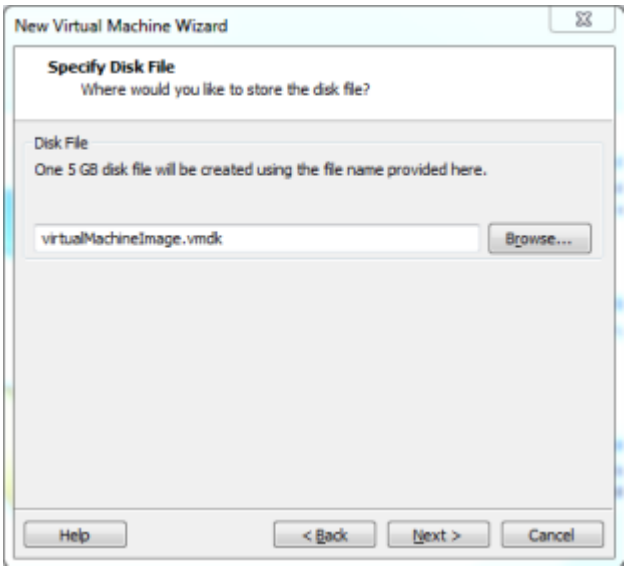
| Step | Details |
|---|---|
| **Step 14:** Specify the details in the **Specify Disk Capacity** window and then click **Next**. | • **Maximum disk size (GB)** — You must enter 5 GB.<br>• Select **Allocate all disk space now**.<br>• Select **Store virtual disk as a single file**.<br>  |
| **Step 15:** In the **Specify Disk file** window, make sure virtualMachineImage.vmdk is displayed by default and click **Next**.<br>If you specified a different name for **Virtual Machine name**, that name is displayed here. |  |

**Table 5-2 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image** *(continued)*

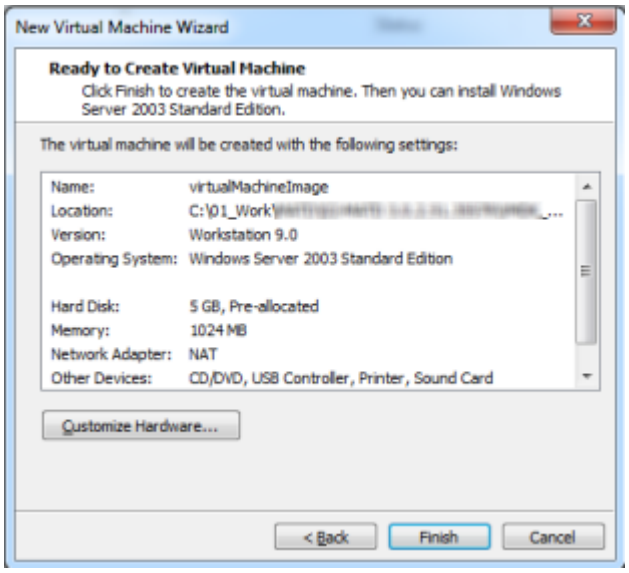
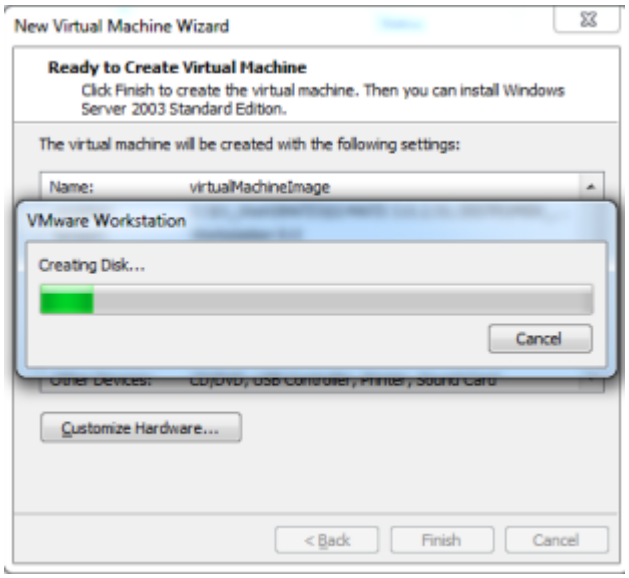
| Step | Details |
|---|---|
| **Step 16:** Review the virtual machine creation settings and click **Finish**. This creates the virtual machine and then you must install the operating system. |  <br>  |

**Table 5-2 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image** *(continued)*

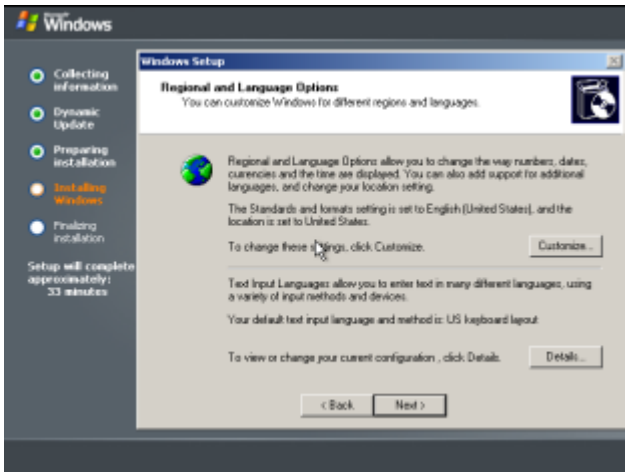
| Step | Details |
|---|---|
| **Step 17:** In the VMware Workstation, power on the virtual machine that you just created and install Windows Server 2003 following the usual procedure.<br>• This step might take around 30 minutes to complete.<br>• You can use the NTFS file system to format the partition during installation.<br>• Do not install VMware Tools. If you did not stop the VMware Tools installation, you can continue with the VMDK file creation process but make sure it is uninstalled when the VMDK file is ready. | |
| **Step 18:** In the **Regional and Language Options** window, you can customize the settings. |  |

**Table 5-2 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image** *(continued)*

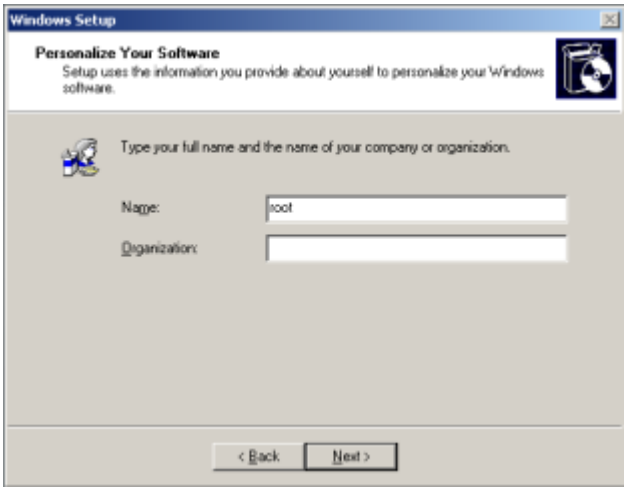
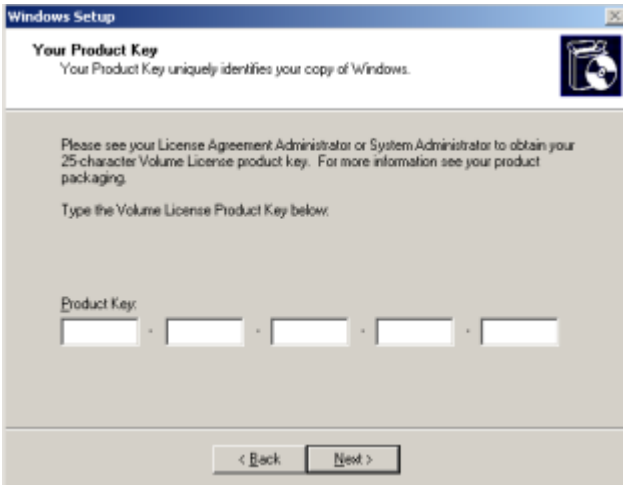
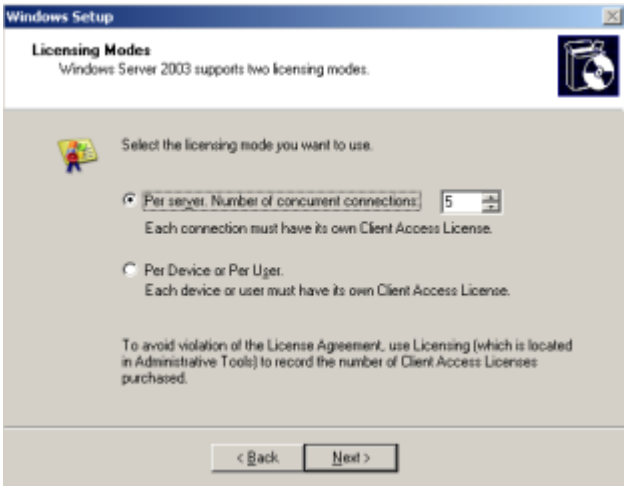
| Step | Details |
|---|---|
| **Step 19:** Enter the following details in the **Windows Setup** window. | • **Name:** Enter `root`<br>• **Organization:** Leave this blank and click **Next.**<br>  |
| **Step 20:** Enter a valid product key and click **Next.** |  |
| **Step 21:** Select **Per Server** licensing mode and enter the valid number of concurrent connections as per your license. |  |

**Table 5-2 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image** *(continued)*

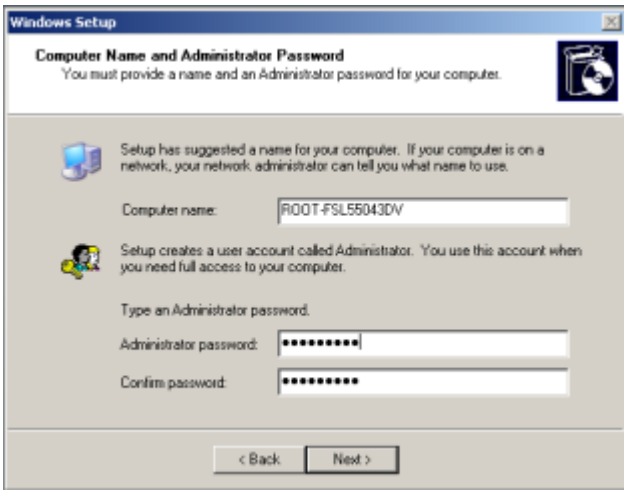
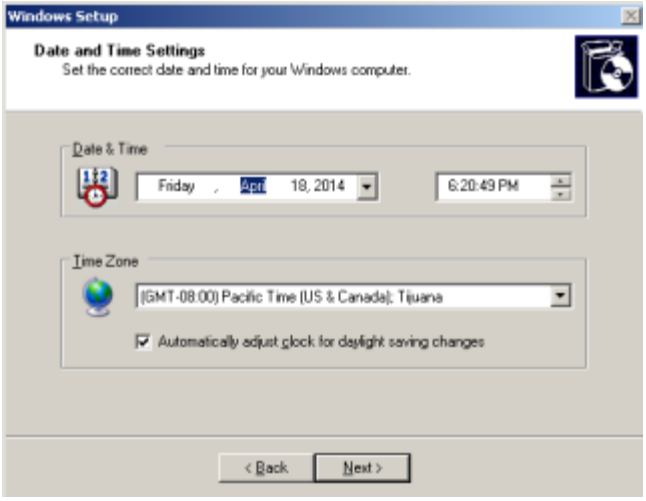
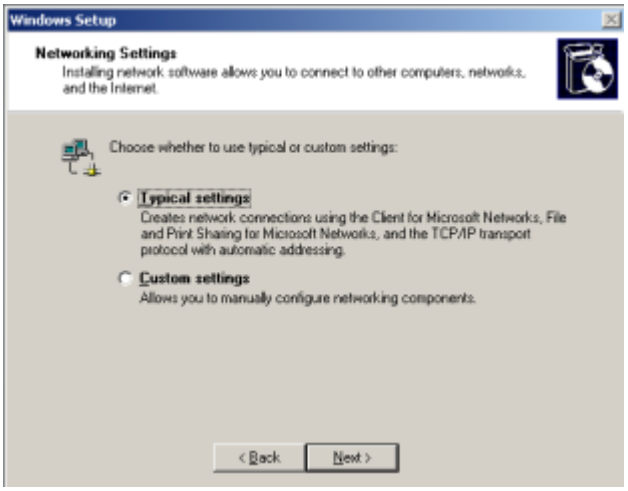
| Step | Details |
|---|---|
| **Step 22:** Enter the following details in the **Computer Name and Administrator Password** window. | • Computer name — leave the default value.<br>• Administrator password — `cr@cker42`<br>• Confirm password — `cr@cker42`<br>  |
| **Step 23:** Click **Next** in the **Date and Time Settings** window. |  |
| **Step 24:** In the **Network Settings** window, leave the default values and click **Next**. |  |

**Table 5-2 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image** *(continued)*

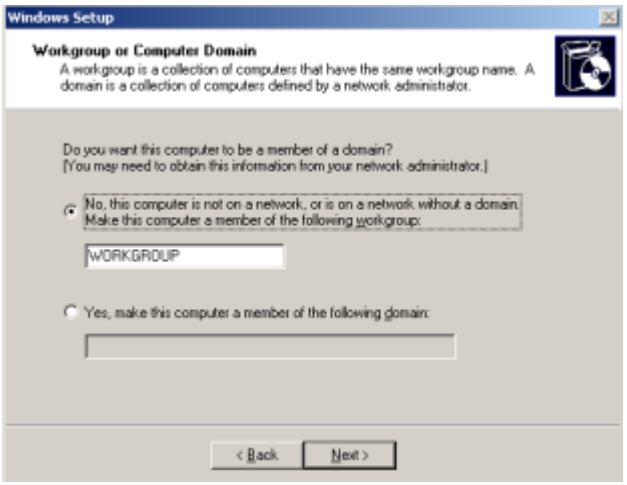
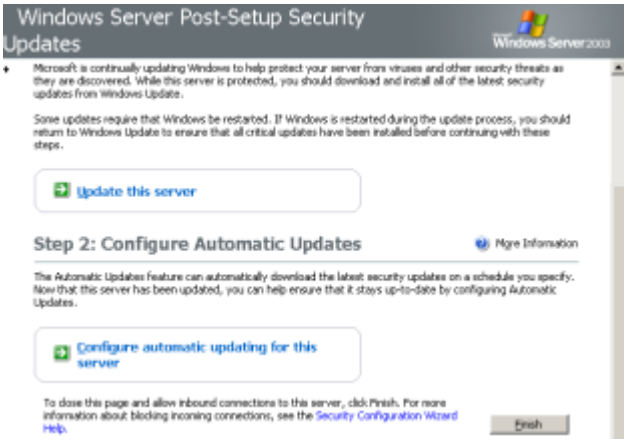
| Step | Details |
|---|---|
| **Step 25:** Leave the default values in the **Workgroup or Computer Domain** window and click **Next**. |  |
| **Step 26:** Log on to the virtual machine with the following credentials. | • **User:** `administrator`<br>• **Password:** `cr@cker42` |
| **Step 27:** If the **Windows Server Post-Setup Security Updates** page is displayed, click **Finish**. |  |
| **Step 28:** If the **Manage Your Server** window is displayed, select **Don't Display the page at logon** and close it. | |

**Table 5-2 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image** *(continued)*

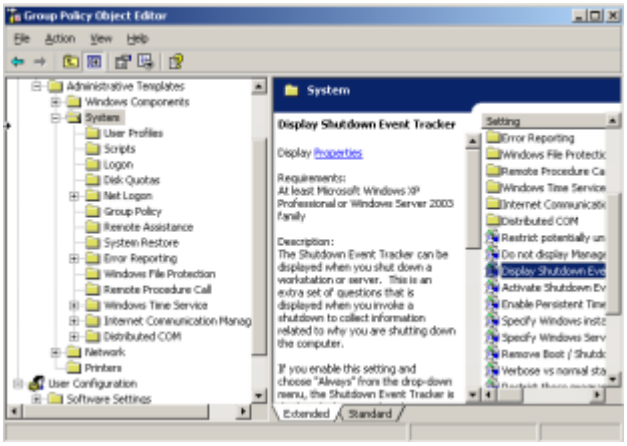
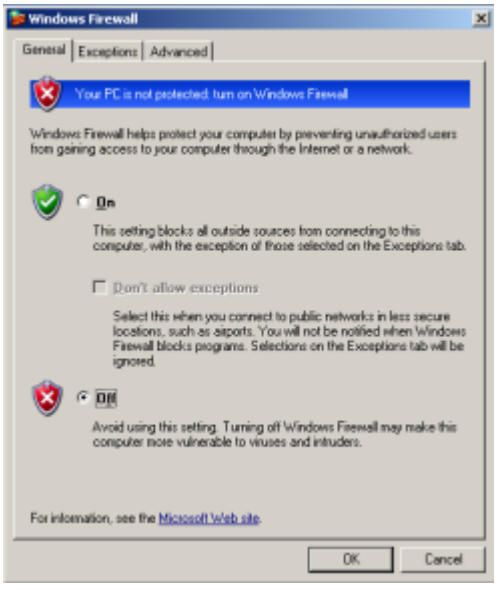
| Step | Details |
|---|---|
| **Step 29:** Complete the following steps. | 1 Select **Start** \| **Run** and enter `gpedit.msc`.<br>2 In the **Group policy object editor** window, select **Computer Configuration** \| **Administrative Templates** \| **System** and double-click **Display Shutdown Event Tracker.**<br>  <br>3 Select **Disabled** and click **OK**.<br>4 Close the **Group policy object editor** window. |
| **Step 30:** Complete the following steps only for Windows Server 2003 SP1. For Windows Server 2003 SP2, you must not execute this step. | 1 Go to http://support.microsoft.com/hotfix/KBHotfix.aspx?kbnum=899260&kbln=en-us and install the hotfix corresponding to your version of Windows Server 2003.<br>2 Restart the computer.<br>3 In the Windows command prompt, enter `tlntsvr /service` and press Enter. |
| **Step 31:** In the virtualMachineImage, select **Start** \| **Control Panel** \| **Windows Firewall** \| **OFF.** |  |

**Table 5-2 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image** *(continued)*

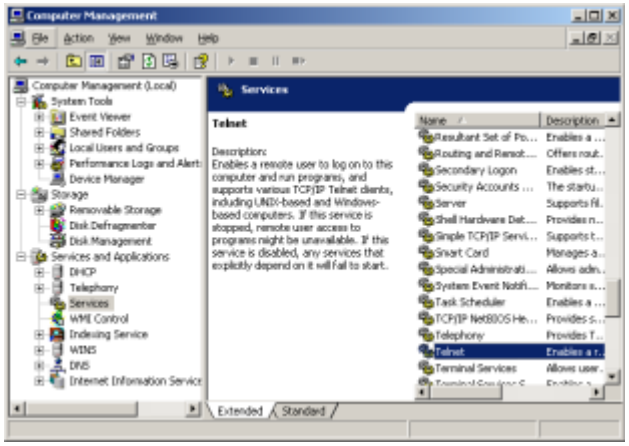
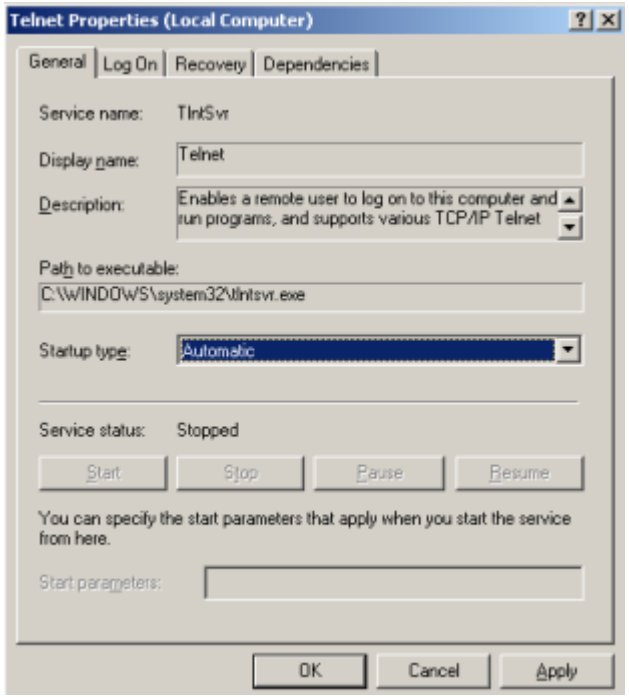
| Step | Details |
|---|---|
| **Step 32:** Click **Start** and right-click **My Computer**. Then select **Manage** \| **Services and Applications** \| **Services**. Then, double-click **Telnet.** |  |
| **Step 33:** In the **Telnet Properties(Local Computer)** window, you must select **Automatic** from the **Startup type** drop-down list. Then select **Apply** \| **Start** \| **OK.** |  |

**Table 5-2 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image** *(continued)*

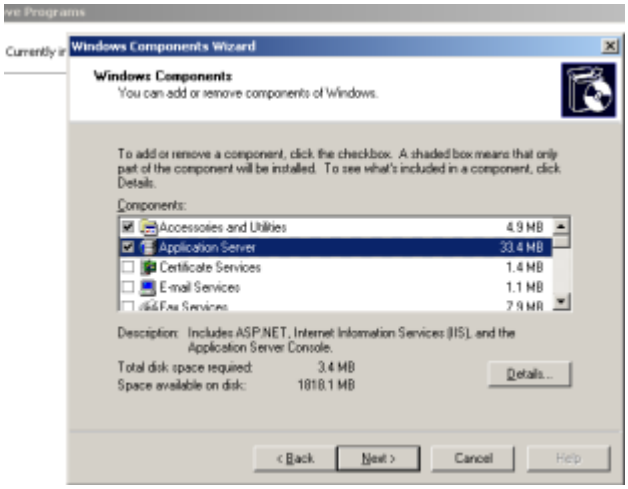
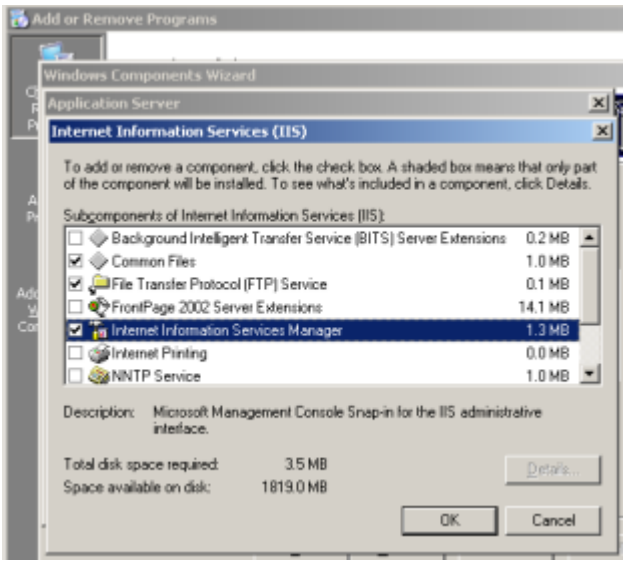
| Step | Details |
|---|---|
| **Step 34:** Enable FTP on the VM. | 1 In the virtualMachineImage, select **Start** \| **Control Panel** \| **Add or remove Programs** \| **Add/Remove Windows components.**<br>  <br><br>2 Double-click **Application Server.**<br>3 Double-click **Internet Information Services(IIS)** |
| **Step 35:** In the **Internet Information Services(IIS)** pop-up window, complete the following. | 1 Select **Common Files.**<br>2 Select **File Transfer Protocol (FTP) Service.**<br>3 Select **Internet Information Services Manager**, click **OK**, and then click **Next** in the **Windows Components Wizard.**<br>  <br> |

**Table 5-2 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image** *(continued)*

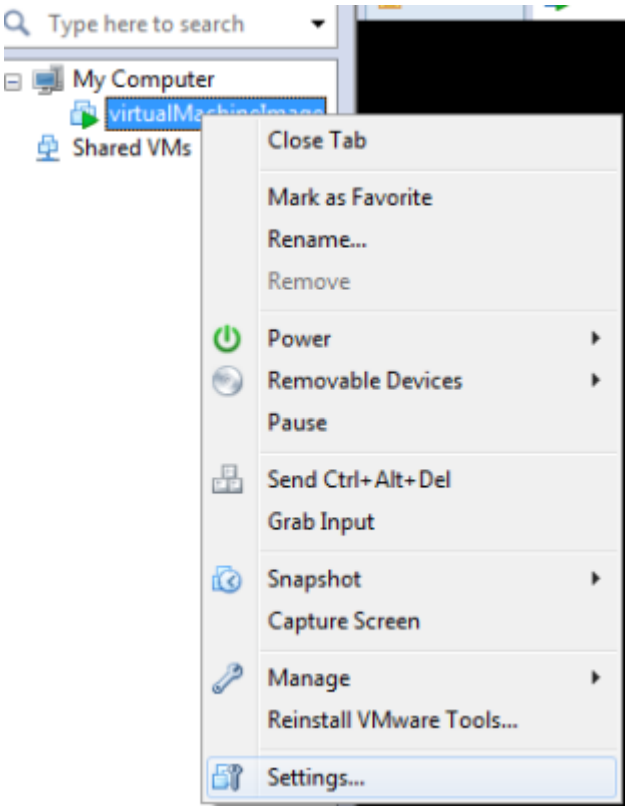
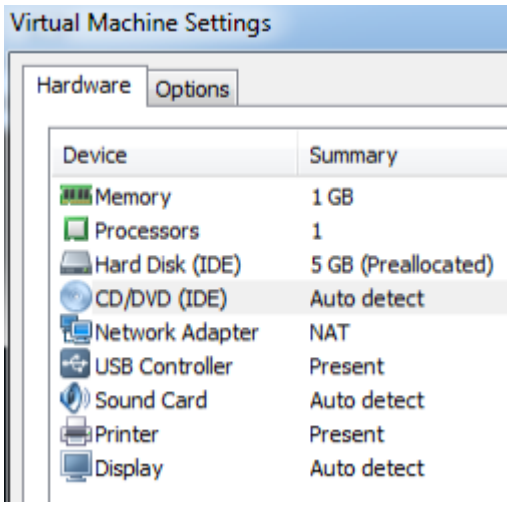
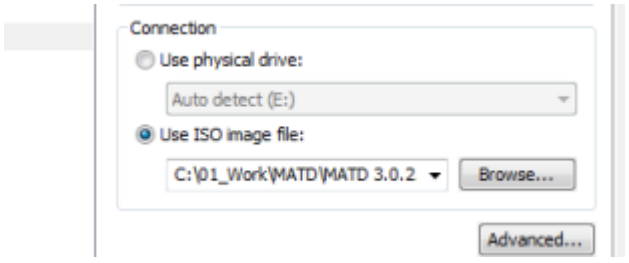
| Step | Details |
|---|---|
| **Step 36:** In the VMware Workstation, right-click on the VM, which in this example is virtualMachineImage. Then, select **Settings**. |  |
| **Step 37:** In the Virtual Machine Settings window, select **CD/DVD (IDE)**. |  |
| **Step 38:** In the **Use ISO image file** field, browse to the ISO file that you used and press **OK**.<br>Close Windows Explorer, if it opens. |  |

**Table 5-2 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image** *(continued)*

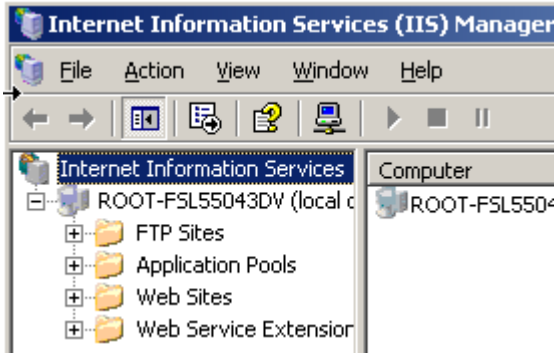
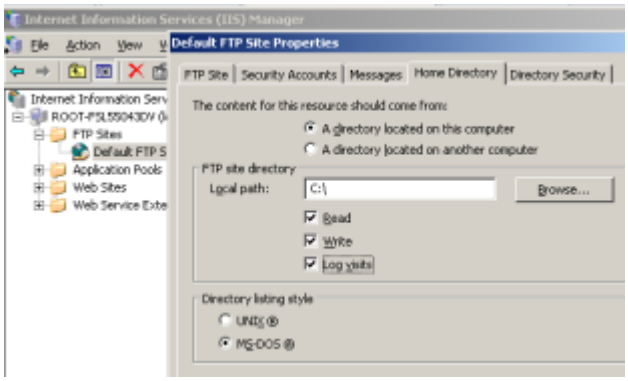
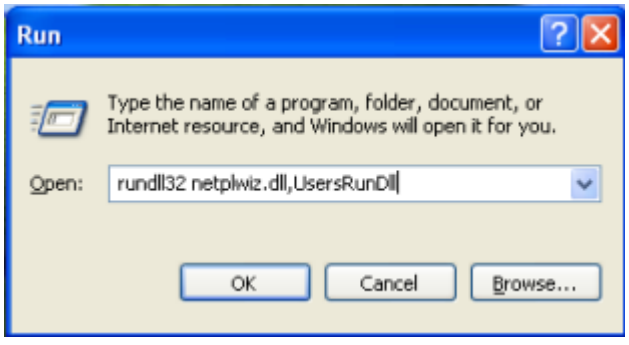
| Step | Details |
|---|---|
| **Step 39:** In the virtualMachineImage, select **Start \| Control Panel \| Administrative Tools \| Internet Information Services (IIS) Manager.** | |
| **Step 40:** In the **Internet Information Services (IIS) Manager** window, expand + below **Internet Information Services.** |  |
| **Step 41:** Complete the following. | 1 Select **FTP Sites** and then right-click **Default FTP Sites.**<br>2 Select **Properties \| Home Directory.**<br>3 Browse to C:\<br>4 Select **Read.**<br>5 Select **Write.**<br>6 Select **Log visits** and click **Apply** and then **OK.**<br>  |
| **Step 42:** Set automatic logon by selecting **Start \| Run**, enter `rundll32 netplwiz.dll,UsersRunDll` and press **Enter**. |  |

**Table 5-2 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image** *(continued)*

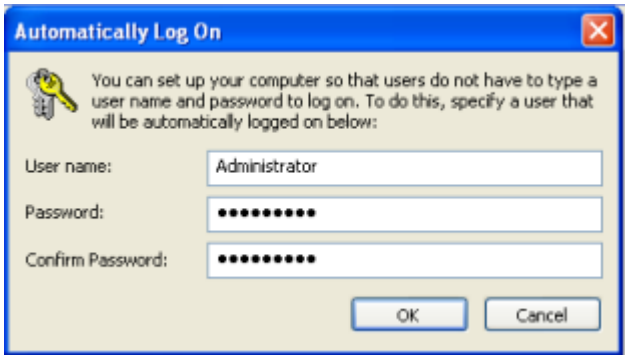
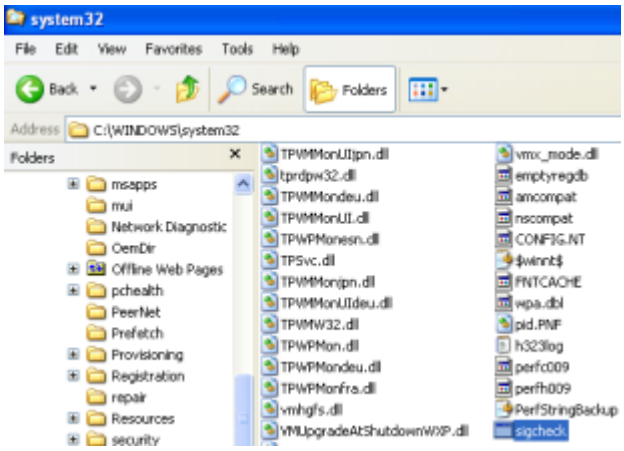
| Step | Details |
|---|---|
| **Step 43:** In the **User Accounts** window, deselect **Users must enter a user name and password to use this computer** and click **Apply**. | |
| **Step 44:** In the **Automatically Log On** pop-up window, complete the following and then press **OK** in the message boxes. | • **User name** — Enter `Administrator`<br>• **Password** — Enter `cr@cker42`<br>• **Confirm Password** — Enter `cr@cker42`<br>  |
| **Step 45:** Download Sigcheck on to your computer (the native host) from http://technet.microsoft.com/en-us/sysinternals/bb897441.aspx. | The VM that you created has the Windows Firewall switch off as well as there is no anti-virus installed on it. Therefore, it is recommended that you download the programs and components on to the native host first and then copy them to the VM in VMware Workstation. |

**Table 5-2 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image** *(continued)*

| Step | Details |
|---|---|
| **Step 46:** Extract sigcheck.zip to `C:\WINDOWS\system32` location. |  |
| **Step 47:** In Windows Explorer, go to C:\ WINDOWS \system32 and double-click **sigcheck.exe**. | |
| **Step 48:** If prompted, click **Run** in the warning message. | |
| **Step 49:** Click **Agree** for **Sigcheck License Agreement**.<br><br>After you click on **Agree**, no confirmation message is displayed. | |
| **Step 50:** Run the MergeIDE batch file on the VM. | 1 Download MergeIDE.zip from https://www.virtualbox.org/attachment/wiki/Migrate_Windows/MergeIDE.zip on to the native computer and then copy it to the VM.<br>2 Extract MergeIDE.zip and run the MergeIDE batch file in the VM.<br>3 If prompted, select **Run** in the warning message.<br>4 Close Windows Explorer. |



SigCheck License Agreement
You can also use the /accepteula command-line switch to accept the EULA.
SYSINTERNALS SOFTWARE LICENSE TERMS
These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Systinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals
updates,
supplements,
Internet-based services, and
Print
Agree
Decline

**Table 5-2 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image** *(continued)*

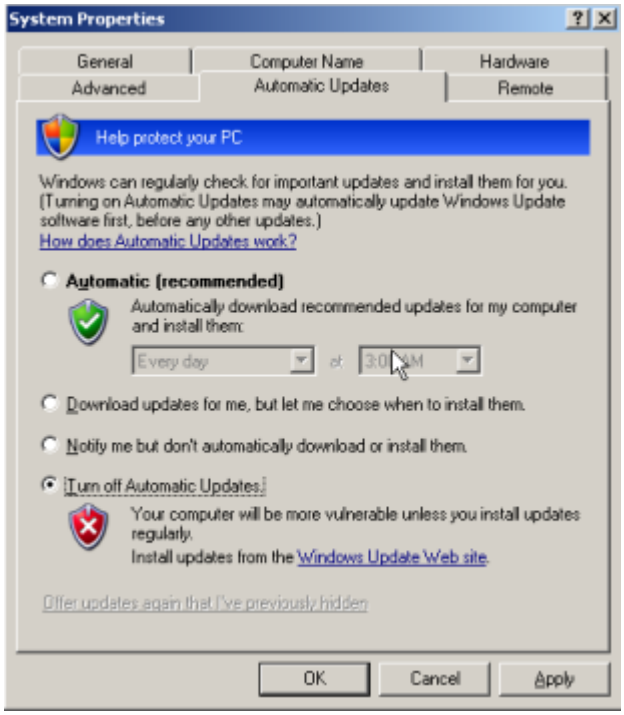
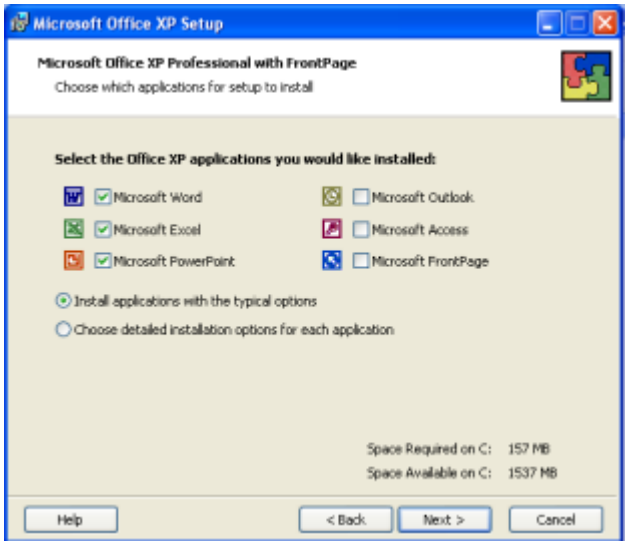
| Step | Details |
|---|---|
| **Step 51:** Disable Windows updates. | 1 Select **Start** \| **Control Panel** \| **System** \| **Automatic Updates.**<br>2 In the **System Properties** window, select **Turn off Automatic Updates.**<br>  <br>3 Click **Apply** and then **OK.** |
| **Step 52:** To analyze Microsoft Word, Excel, and Powerpoint files, install Microsoft Office 2003 on the virtual machine. |  |

**Table 5-2 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image** *(continued)*

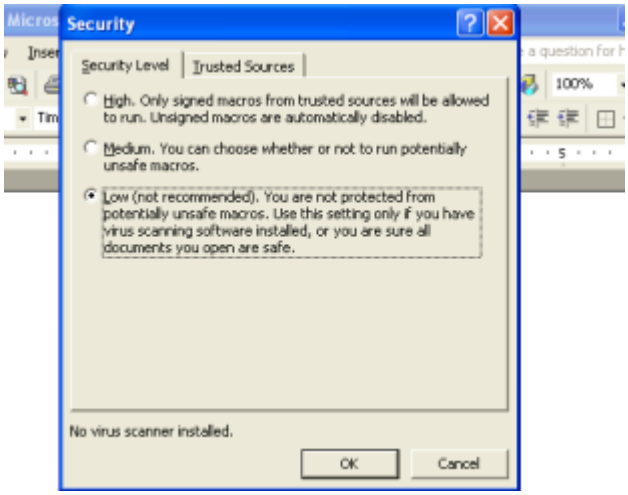
| Step | Details |
|---|---|
| **Step 53:** Lower the security to run macros for the Office applications. | • Open Microsoft Word 2003 and select **Tools** \| **Macro** \| **Security** and then select **Low** and click **OK**.<br>  <br>• Similarly lower the macro security for Microsoft Excel and Powerpoint. |
| **Step 54:** You need the compatibility pack to open Microsoft Office files that were created in a newer version of Microsoft Office. For example, to open a .docx file using Office 2003, you need the corresponding compatibility pack installed.<br>Go to http://www.microsoft.com/en-us/download/details.aspx?id=3 and download the required Microsoft Office compatibility pack for Word, Excel, and PowerPoint File Formats. Then install them on the virtual machine. | |

**Table 5-2 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image** *(continued)*

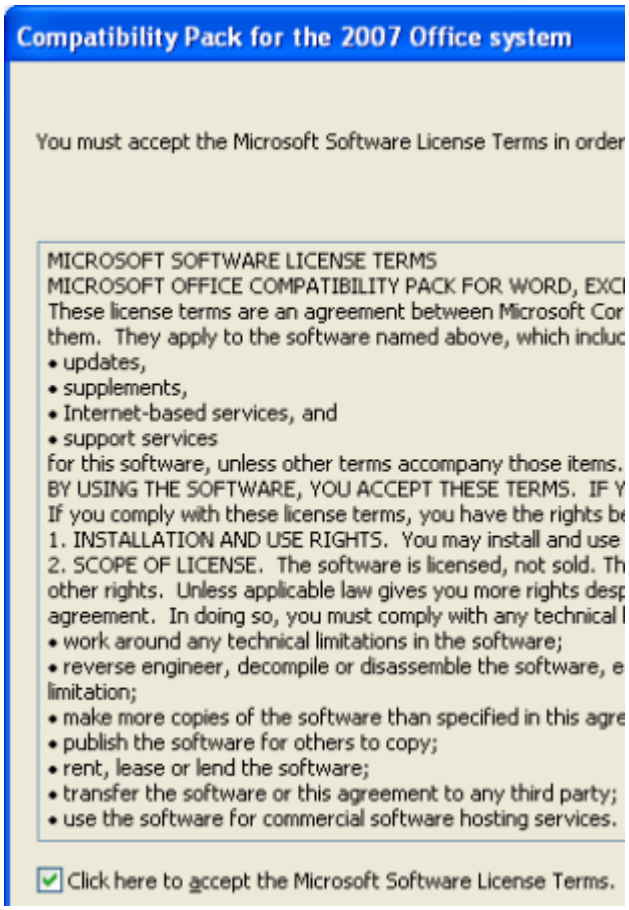
| Step | Details |
|---|---|
| **Step 55:** In the **Compatibility Pack for the 2007 Office system** dialog, select **Click here to accept the Microsoft Software License Terms** and click **OK**. |  |

**Table 5-2 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image** *(continued)*

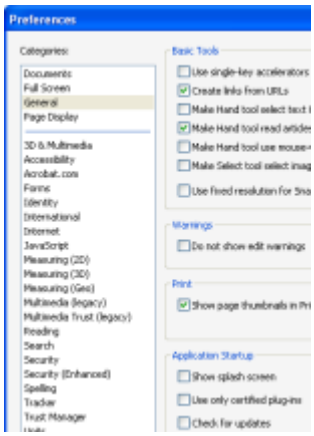
| Step | Details |
|---|---|
| **Step 56:** To analyze PDF files, download Adobe Reader to the native host and copy it to the VM.<br><br>This procedure uses Adobe Reader 9.0 as an example. | 1 Install Adobe Reader 9.0 in the VM.<br>2 Open Adobe Reader and click **Accept**.<br> <br>3 In Adobe Reader, select **Edit** \| **Preferences** \| **General** and deselect **Check for updates**.<br>  |
| **Step 57:** Download the following on to the native host and then install them on the VM. | 1 Download Microsoft Visual C++ 2005 Redistributable Package (x86) from http://www.microsoft.com/en-us/download/details.aspx?id=3387and install it.<br>2 Download Microsoft Visual C++ 2008 Redistributable Package (x86) from http://www.microsoft.com/en-us/download/details.aspx?id=5582and install it.<br>3 Download Microsoft Visual C++ 2010 Redistributable Package (x86) from http://www.microsoft.com/en-us/download/details.aspx?id=5555and install it.<br>4 Download Microsoft .NET Framework 2.0 Service Pack 2 (x86 version) from http://www.microsoft.com/en-us/download/details.aspx?id=1639and install it. |

**Table 5-2 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image** *(continued)*

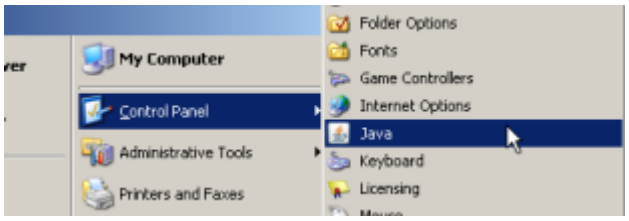
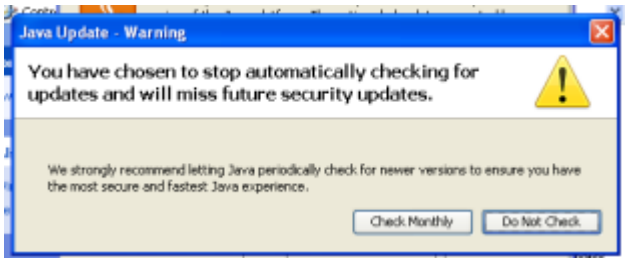
| Step | Details |
|---|---|
| **Step 58:** To analyze JAR files, download and install Java Runtime Environment.<br><br>This procedure uses Java 7 Update 25 as an example. | |
| **Step 59:** Open Java in the Control Panel. |  |
| **Step 60:** In the **Update** tab, deselect **Check for Updates Automatically.** | |
| **Step 61:** In the Java Update Warning dialog, select **Do Not Check** and then click **OK** in the Java Control Panel. |  |

**Table 5-2 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image** *(continued)*

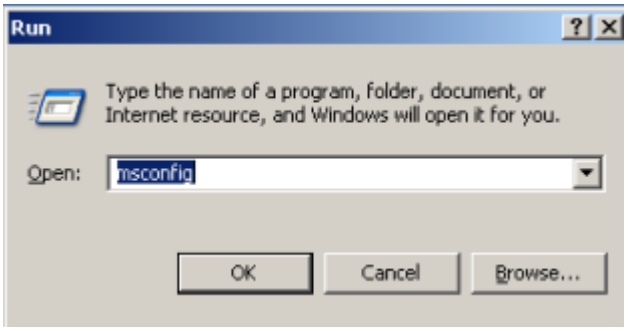
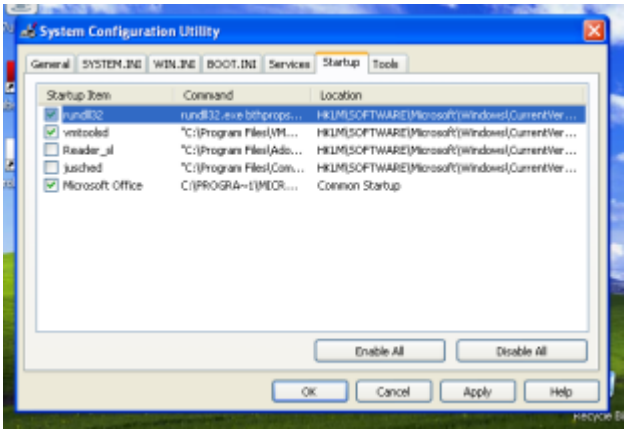
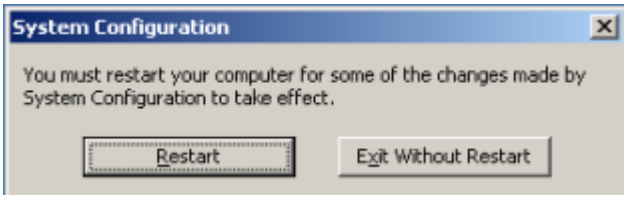
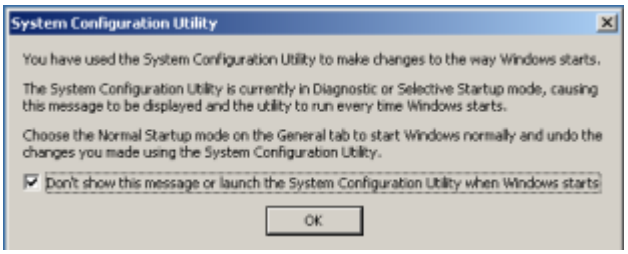
| Step | Details |
|---|---|
| **Step 62:** In the Windows Run dialog, enter `msconfig`. |  |
| **Step 63:** In the System Configuration utility, go to the **Startup** tab. |  <br>Deselect *reader_sl* and *jusched* and then click **OK**.<br>reader_sl is displayed only if you have installed Adobe Reader. |
| **Step 64:** In the **System Configuration** dialog, click **Restart**. |  |
| **Step 65:** In the **System Configuration Utility** dialog, select **Don't show this message or launch the System Configuration Utility when Windows starts** and click **OK**. |  |

**Table 5-2 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image** *(continued)*

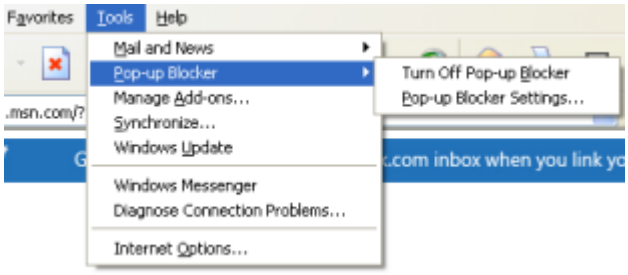
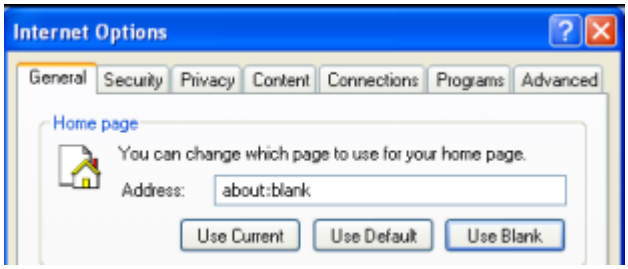
| Step | Details |
|---|---|
| **Step 66:** Open the default browser and set it up for malware analysis.<br><br>This procedure uses Internet Explorer as an example. | 1 Ensure the pop-up blocker is turned off. In Internet Explorer, select **Tools** \| **Pop-up Blocker** \| **Turn off Pop-up Blocker.**<br><br>  <br><br>2 Select **Tools** \| **Internet Options** and for **Home page** select **Use Blank** or **Use new tab** based on the version of Internet Explorer.<br><br>  <br><br>3 Go to the **Advanced** tab of the Internet Options and locate **Security.**<br><br>4 Select **Allow active content to run in files on My Computer.** |

**Table 5-2 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image** *(continued)*

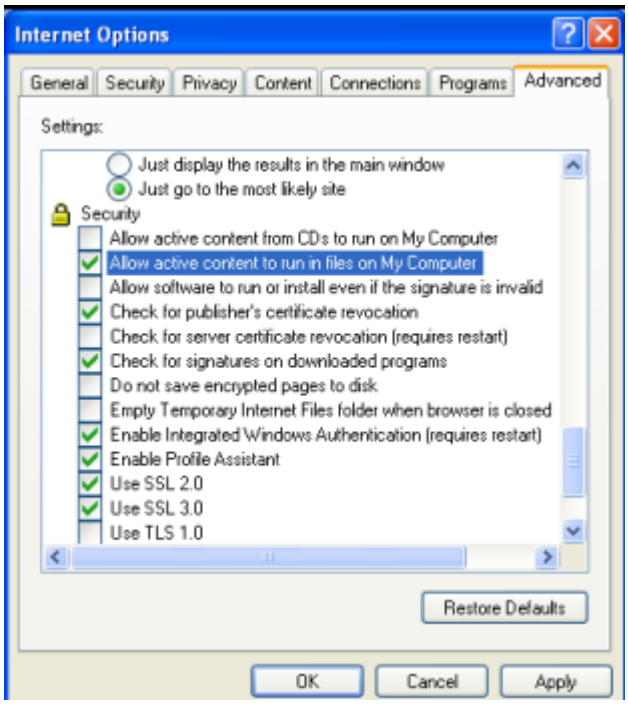
| Step | Details |
|---|---|
| |  <br>**5** Click **OK**. |

**Table 5-2 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image** *(continued)*

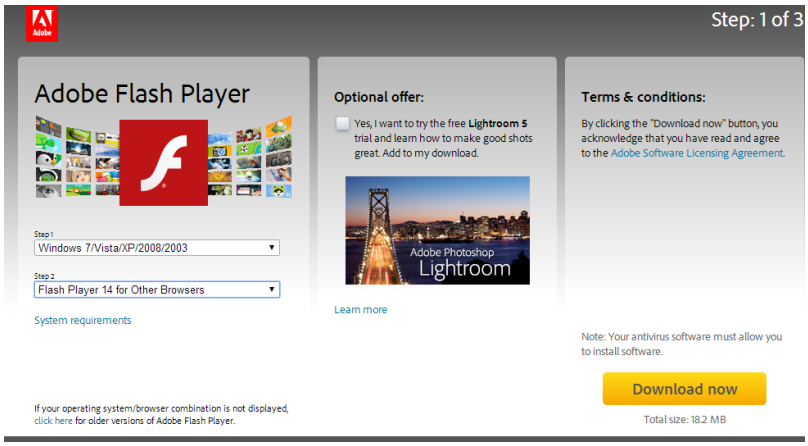
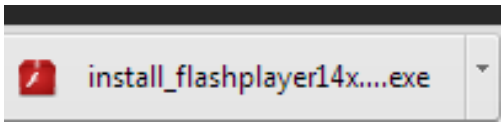
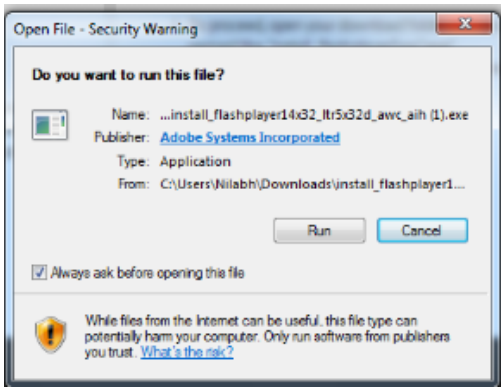
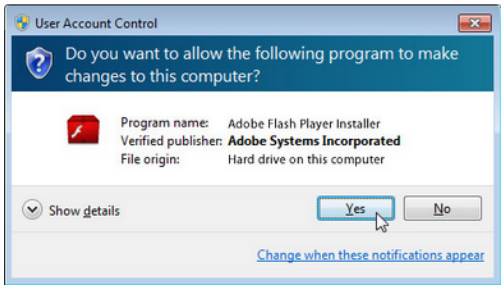
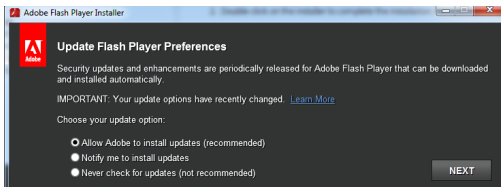
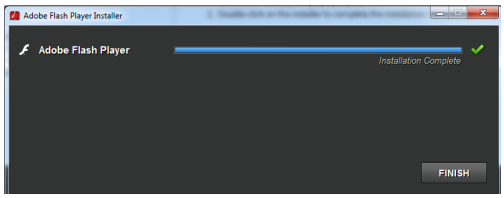
| Step | Details |
|---|---|
| **Step 67:** To dynamically analyze Flash files (SWF), download the required version of Adobe Flash.<br><br>This procedure uses Flash Player 14 as an example. | 1 Goto http://get.adobe.com/flashplayer/otherversions/.<br><br>2 Select Operating System and Flash Player version respectively as per your requirement in **Step 1** and **Step 2** drop-down as shown below.<br><br>3 Click on **Download now** tab.<br><br>  <br><br>4 Double-click the Adobe Flash Player Installer file **(install_flashplayer xxx.exe)**, present at the bottom corner of your screen.<br><br>  <br><br>5 In the**Security Warning dialogue box**, Click **Run**.<br><br>  <br><br>6 In the **User Account Control** dialogue box, Click **Yes**. |

**Table 5-2 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image** *(continued)*

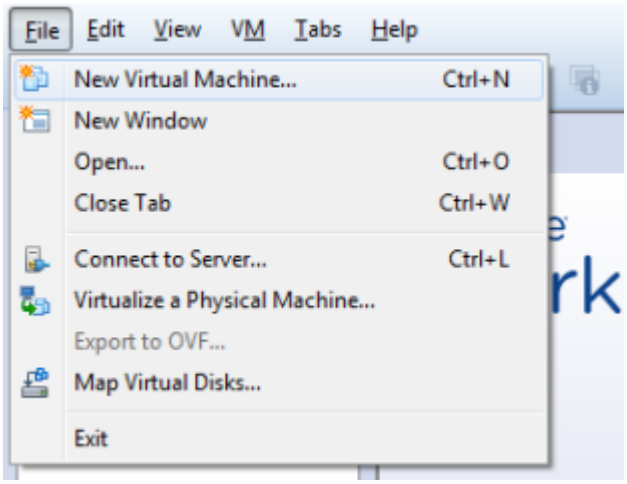
| Step | Details |
|---|---|
| |  <br>7 Choose your update option and Click **NEXT**.<br>  <br>8 Click **FINISH** to complete Adobe Flash Player installation.<br>  |
| **Step 68:** Shut down virtualMachineImage by selecting **Start** \| **Shut down** \| **Shut down** \| **OK**. | |
| **Step 69:** Go to the location that you provided in step 7 to find the VMDK file named as `virtualMachineImage-flat.vmdk` | |

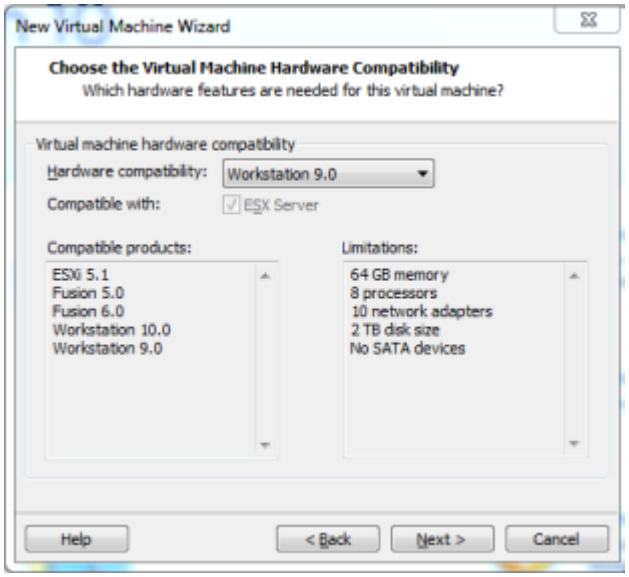
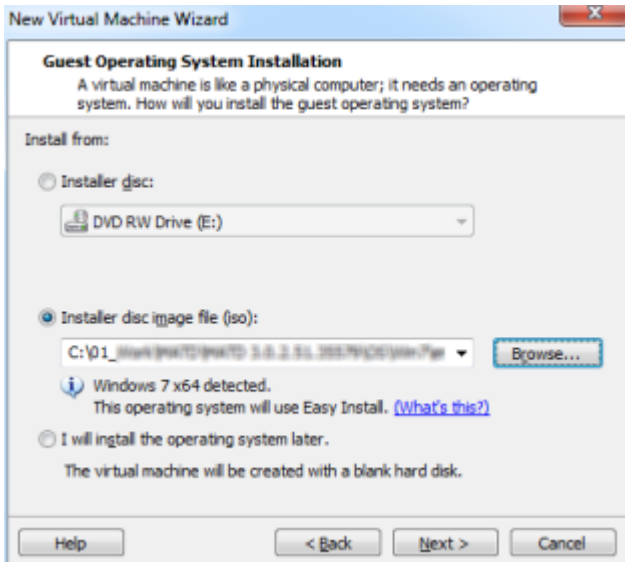
# Create a VMDK file for Windows 7

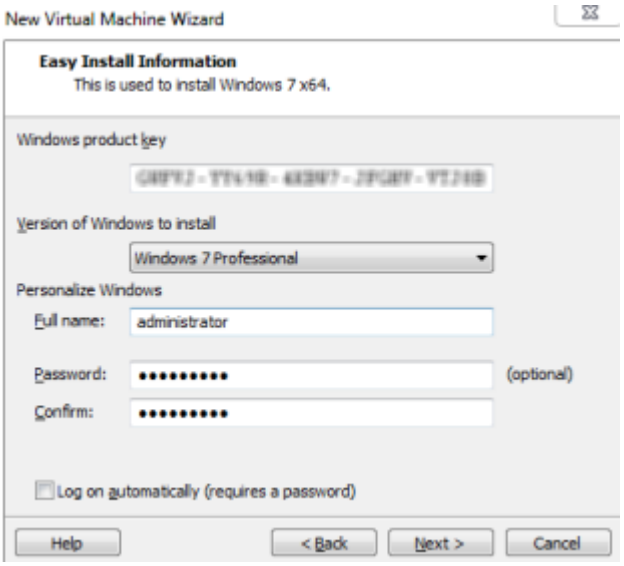
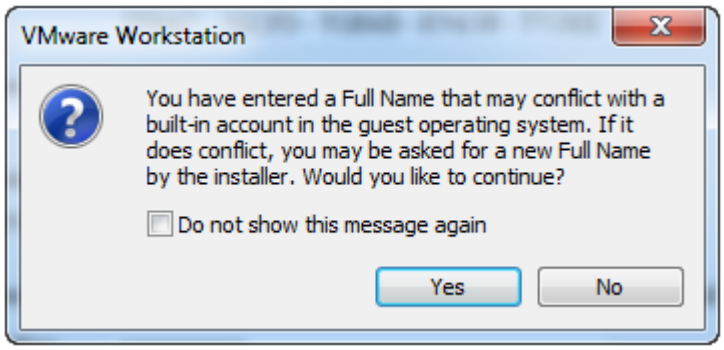
**Before you begin**

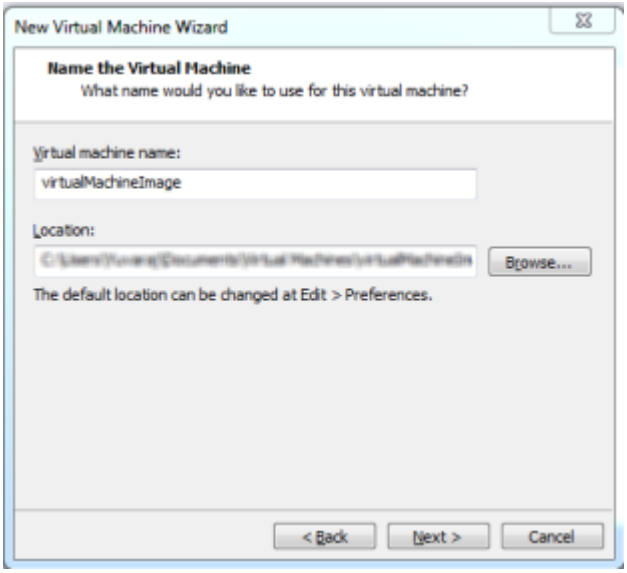
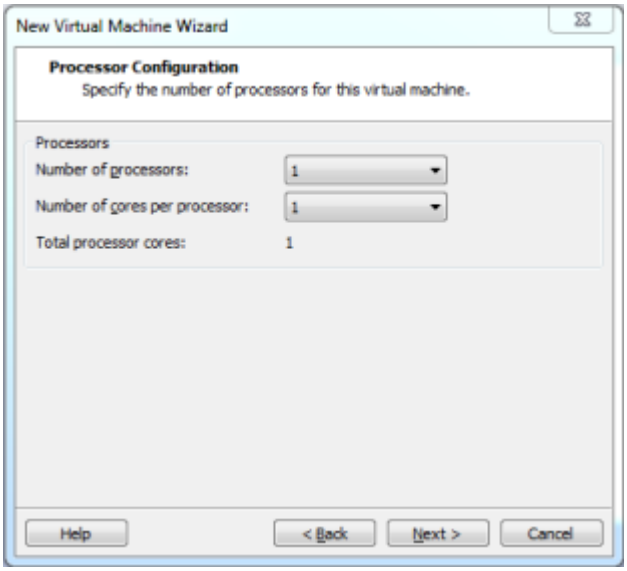
- Download VMware Workstation 9.0 or above from http://www.vmware.com/products/workstation/workstation-evaluation and install it.
- Make sure you have the ISO image of the operating system whose VMDK file you need to create.
- Make sure you have the license key for the operating system.

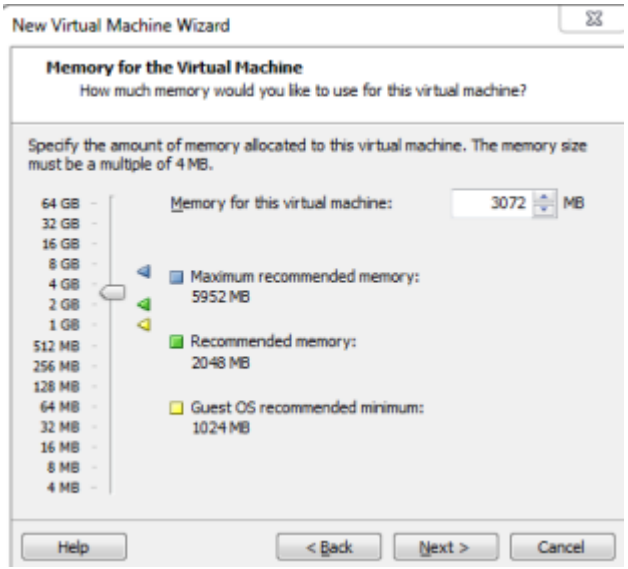
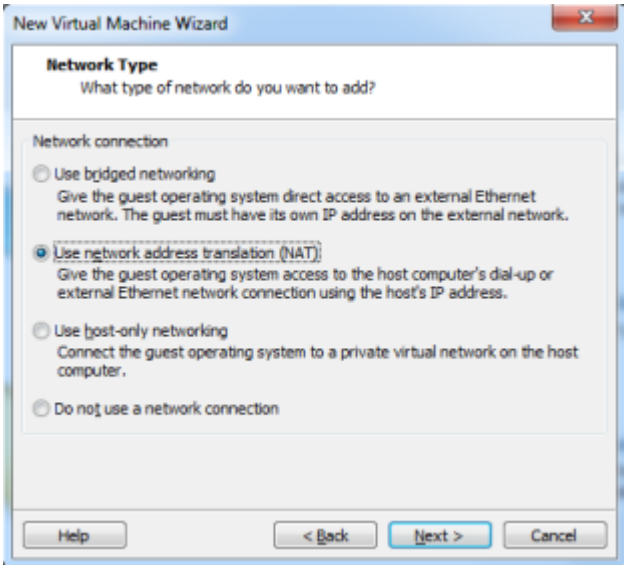
Use this procedure to create VMDK files from an ISO image of Windows 7 SP1 32 or 64 bit.

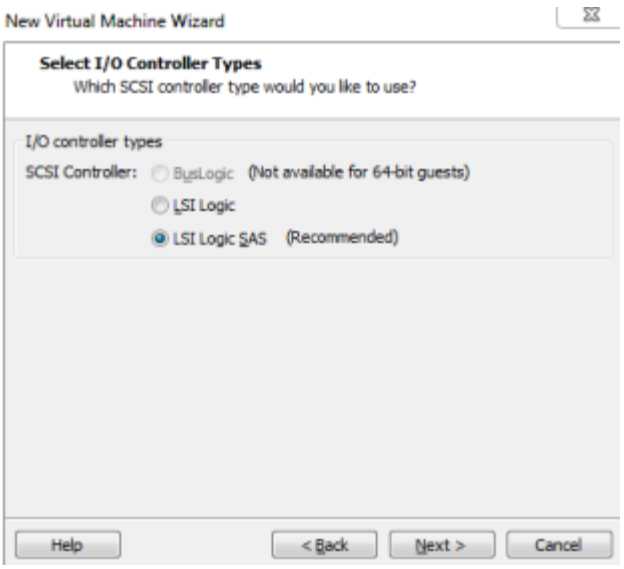
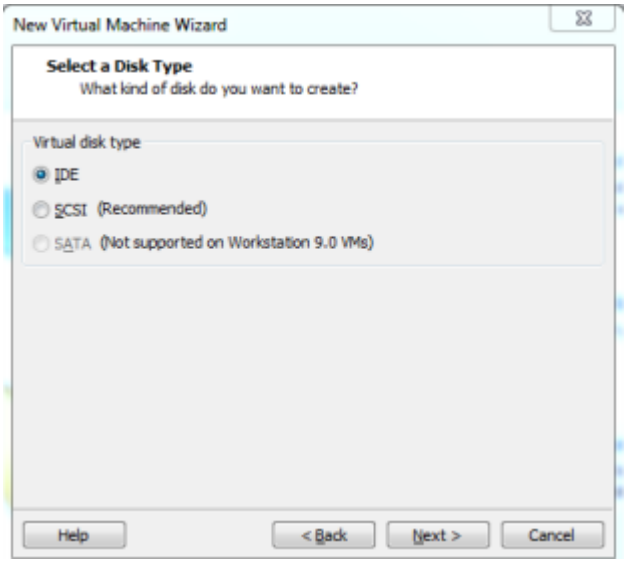
| Step | Details |
|---|---|
| **Step 1:** Start the VMware Workstation. | This procedure uses VMware Workstation 10 as an example. |
| **Step 2:** In the VMware Workstation page, select **File \| New Virtual Machine.** |  |
| **Step 3:** In the **New Virtual Machine Wizard** window, select **Custom (Advanced)** and click **Next.** | |

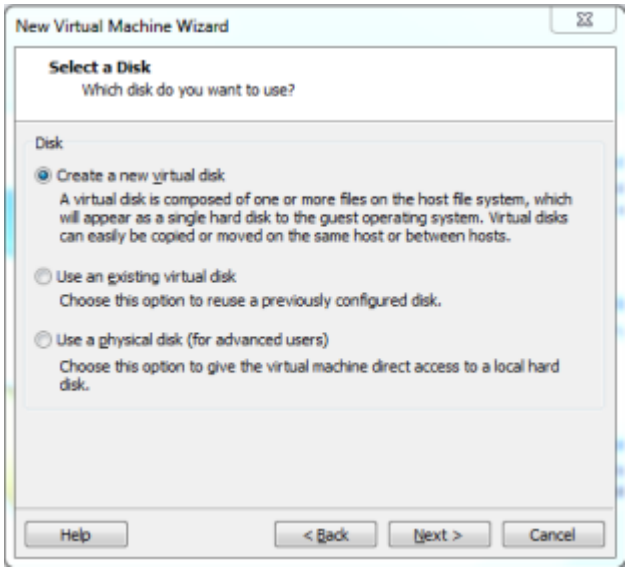
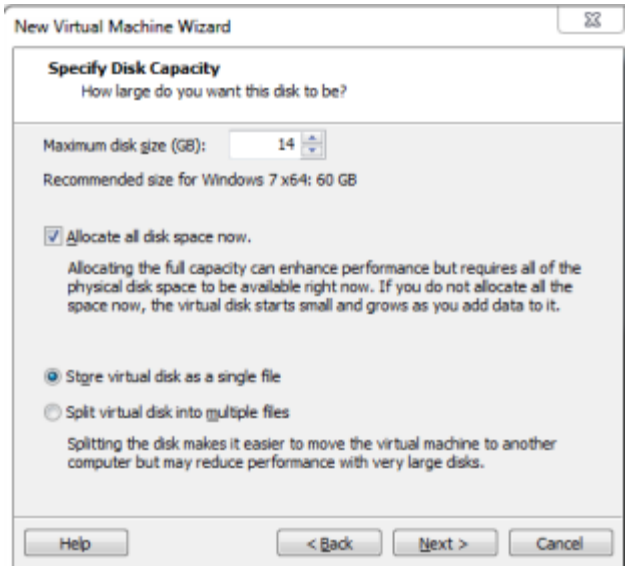
| Step | Details |
|---|---|
| **Step 4:** In the **Choose the Virtual Machine Hardware Compatibility** window, select **Workstation 9.0** from the **Hardware compatibility** drop-down list. For other fields, leave the default values and click **Next**. |  |
| **Step 5:** In the **Guest Operating System Installation** window, select either **Installer disc** or **Installer disc image file (iso)**, browse and select the ISO image, and then click **Next**. |  |

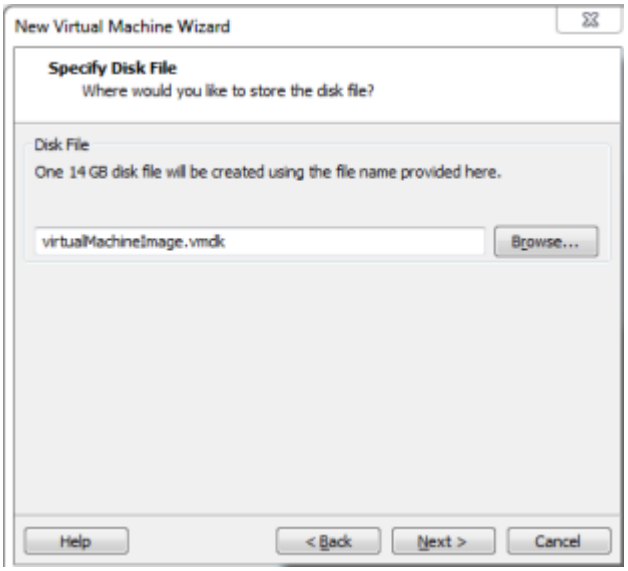
| Step | Details |
|---|---|
| **Step 6:** Enter the information in the **Easy Install Information** window and then click **Next**. | • **Windows product key** — Enter the license key of the Windows operating system for which you are creating the VMDK file.<br>• **Full name** — You must enter `administrator` as the **Full name**.<br>• **Password** — You must enter `cr@cker42` as the password. This is the password that McAfee Advanced Threat Defense uses to log on to the VM.<br>• **Confirm** — Enter `cr@cker42` again to confirm.<br>• **Log on automatically (requires a password)** — Deselect this box.<br>  |
| **Step 7:** If the **VMware Workstation** message displays, click **Yes**. |  |

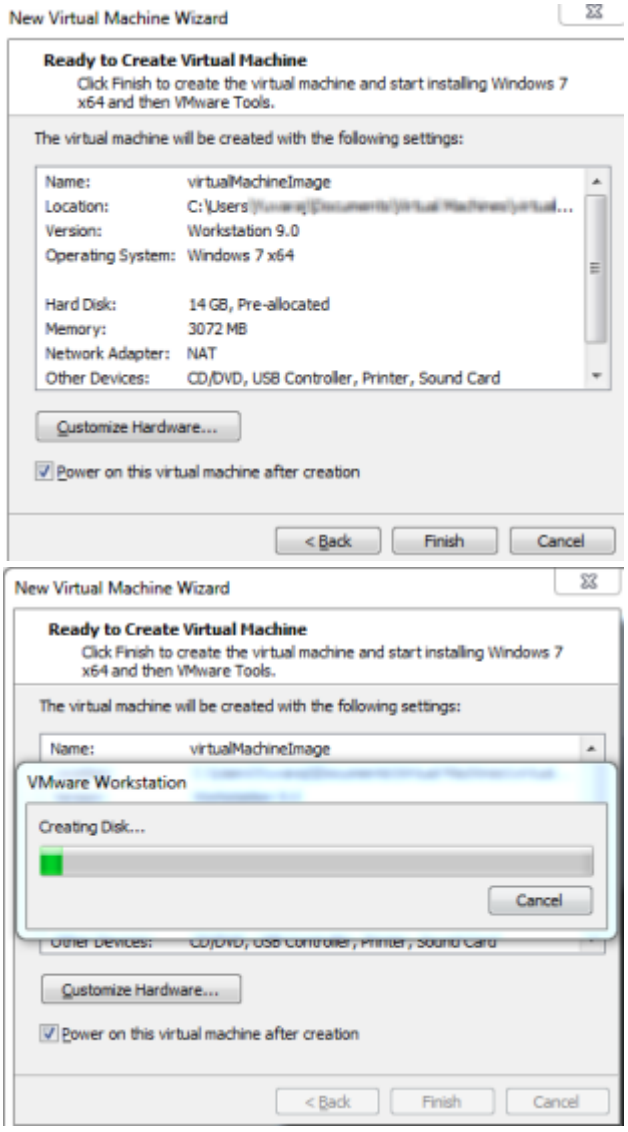
| Step | Details |
|---|---|
| **Step 8:** Enter the information in the **Name the Virtual Machine** window and then click **Next**. | • **Virtual Machine name** — You must enter `virtualMachineImage` as the name.<br>• **Location** — Browse and select the folder where you want to create the VMDK file.<br>  |
| **Step 9:** In the **Processor Configuration** window, leave the default values and click **Next**. |  |

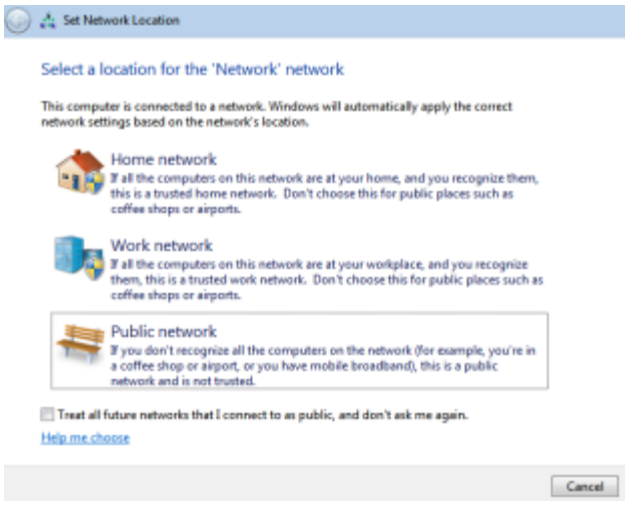
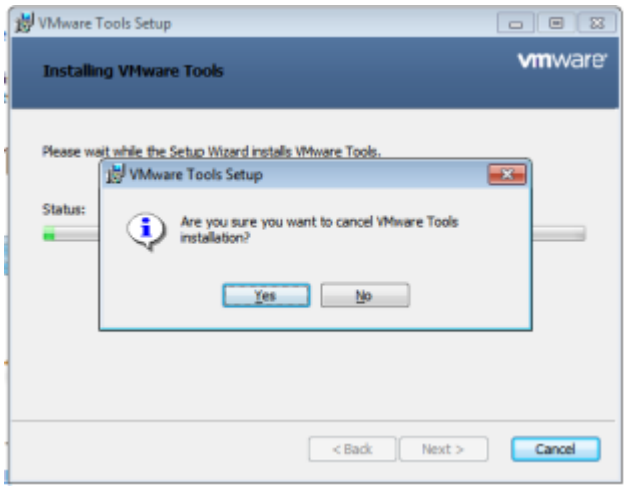
| Step | Details |
|---|---|
| **Step 10:** In the **Memory for the Virtual Machine** window, set 3072 MB as the memory. |  |
| **Step 11:** In the **Network Type** window, leave the default selection. |  |

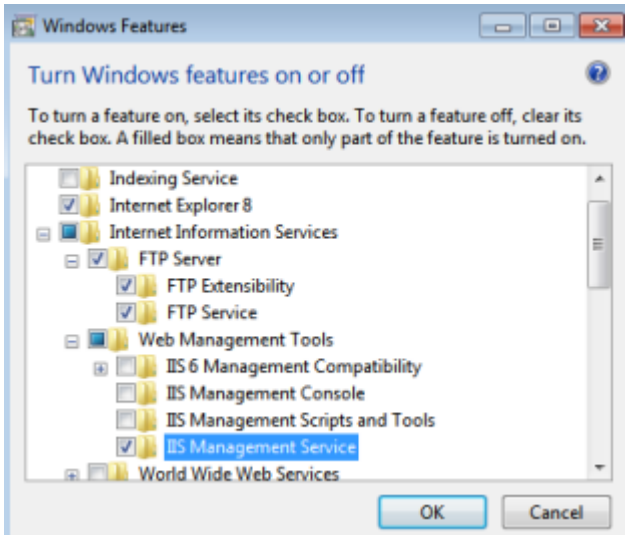
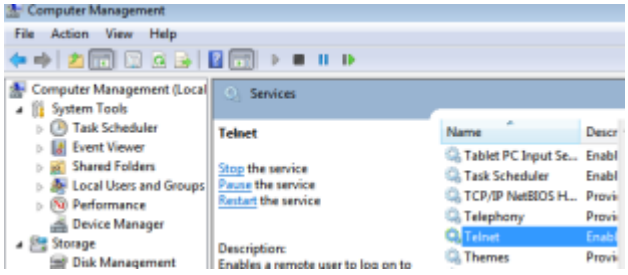
| Step | Details |
|---|---|
| **Step 12:** In the **Select I/O Controller Types** , leave the default selection. |  |
| **Step 13:** In the **Select a Disk Type** page, select **IDE** and click **Next**.<br><br>SCSI disks are not compatible with McAfee Advanced Threat Defense. |  |

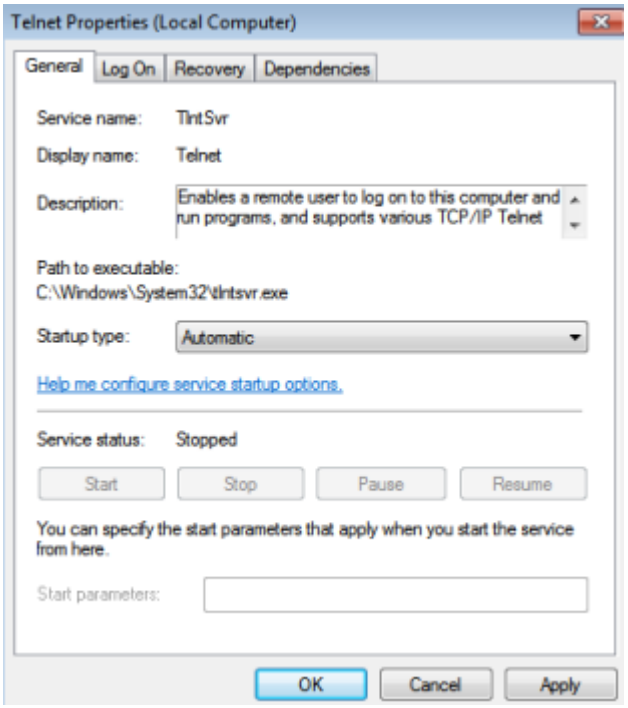
| Step | Details |
|---|---|
| **Step 14:** In the **Select a Disk** window, select **Create a new virtual disk** and click **Next**. |  |
| **Step 15:** Specify the details in the **Specify Disk Capacity** window and then click **Next**. | • **Maximum disk size (GB)** — For Windows 7 64-bit, you must enter, 14 GB. For Windows 7 32-bit, you must enter 12 GB.<br>• Select **Allocate all disk space now**.<br>• Select **Store virtual disk as a single file**.<br>  |

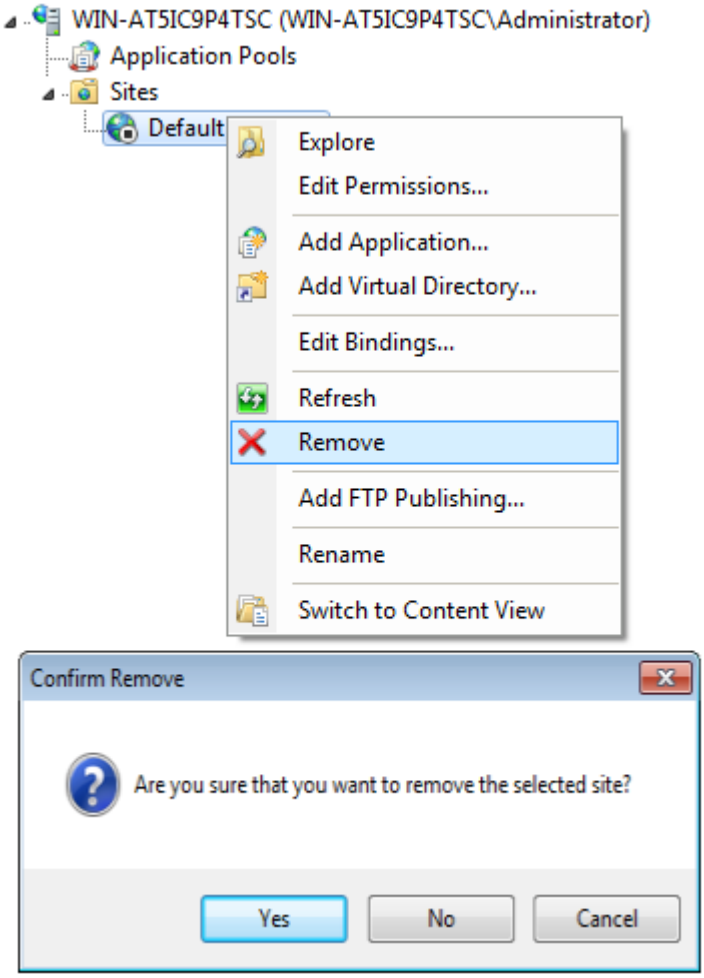
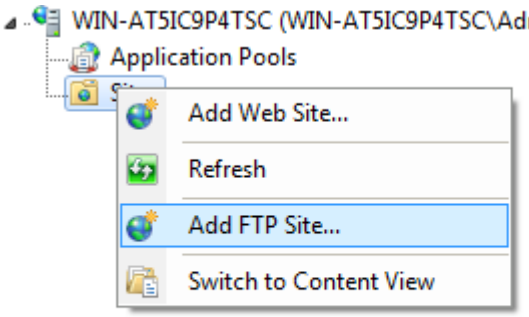
| Step | Details |
|---|---|
| **Step 16:** In the **Specify Disk file** window, make sure virtualMachineImage.vmdk is displayed by default and click **Next**.<br>If you specified a different name for **Virtual Machine name**, that name is displayed here. |  |

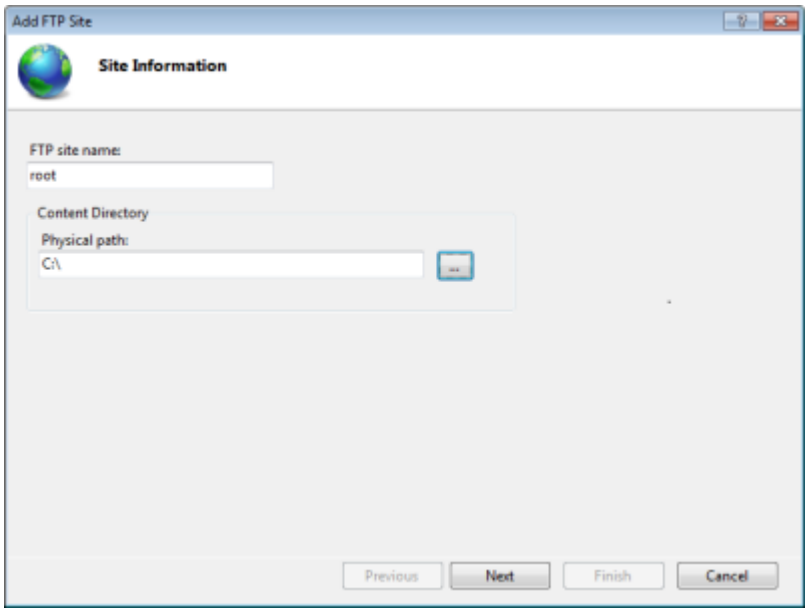
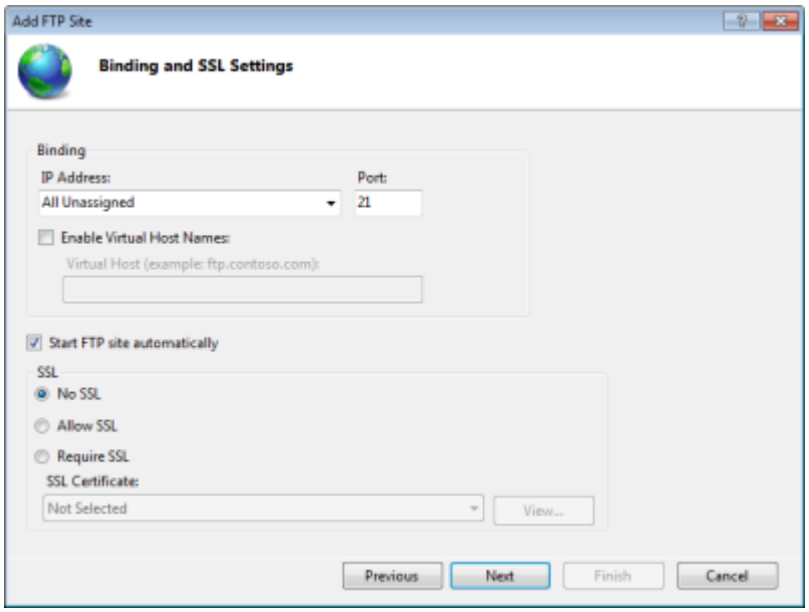
| Step | Details |
|---|---|
| **Step 17:** Complete the following in the **Ready to Create Virtual Machine** window. | • **Power on this virtual machine after creation** — Select this option.<br>• Click **Finish.**<br>This step might take around 30 minutes to complete.<br>  |
| **Step 18:** If the **Removable Devices** pop-up window is displayed, select **Do not show this hint again** and click **OK**. | Windows begins to install, which might take around 15 minutes. |

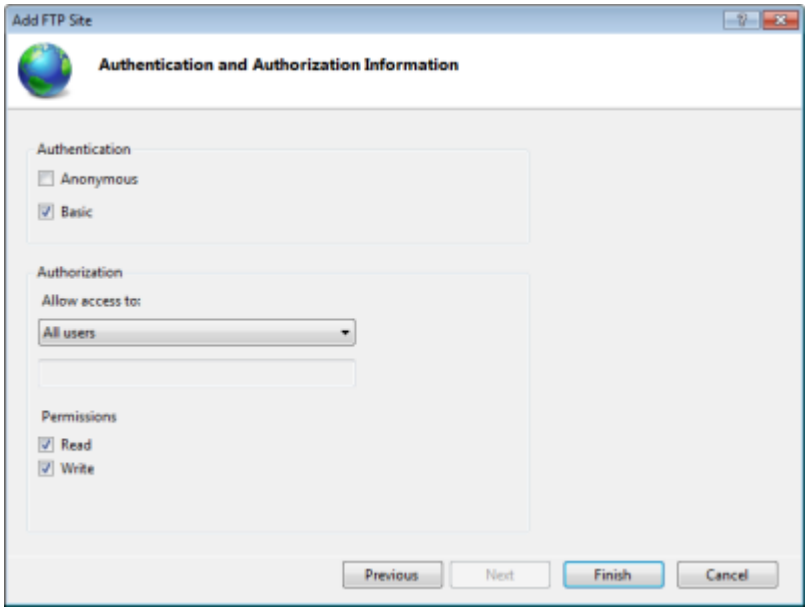
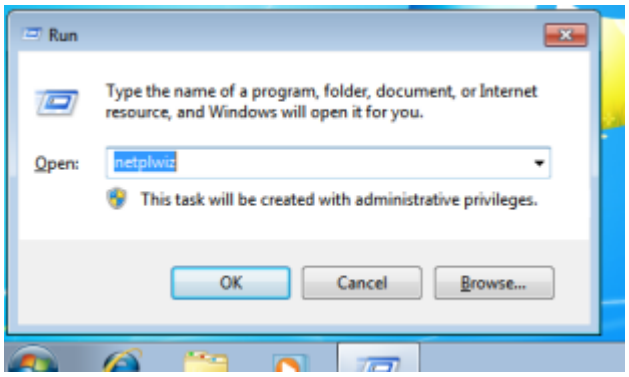
| Step | Details |
|---|---|
| Step 19: If the **Set Network Location** window is displayed, select **Public Network** and select **Close**. |  |
| **Step 20:** Stop the VMware Tools installation.<br>The VMware Tools are not compatible with McAfee Advanced Threat Defense. If you did not stop the VMware Tools installation, you can continue with the VMDK file creation process but make sure it is uninstalled when the VMDK file is ready. |  |
| **Step 23:** In the VM, turn off the Windows Firewall. | 1 Select **Start** \| **Control Panel** \| **System and Security** \| **Windows Firewall** \| **Turn on Windows Firewall On or Off**<br>2 Select **Turn off Windows Firewall (not recommended)** for both **Home or work(private) network location settings** and **Public network location settings** and then click **OK**.<br> |

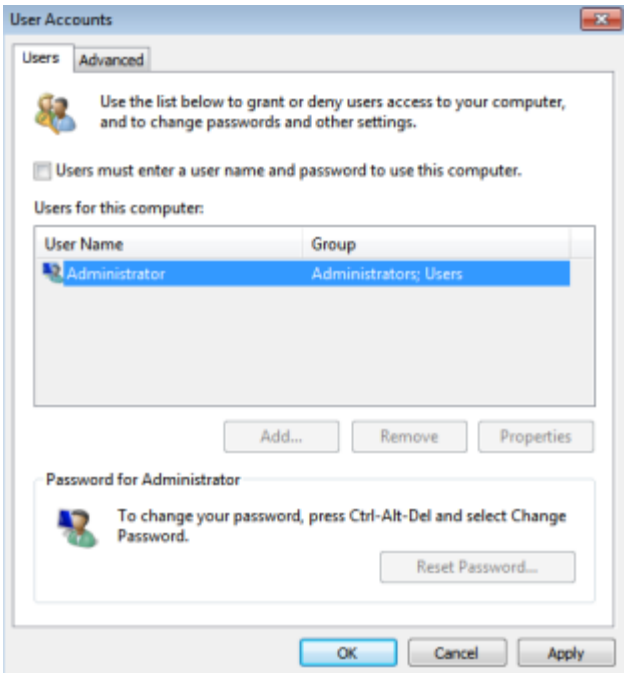
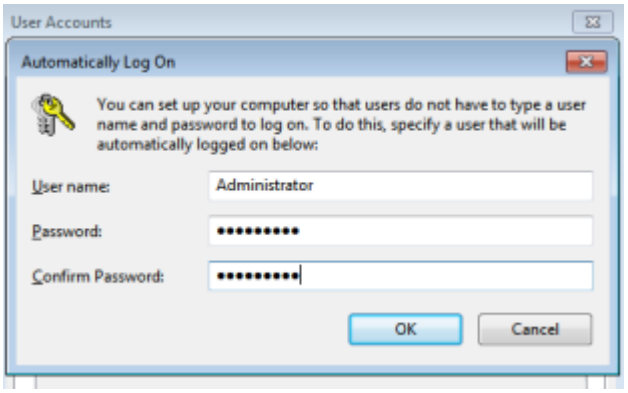
| Step | Details |
|---|---|
| **Step 24:** Select **Start** \| **Control Panel** \| **Programs** \| **Programs and Features** \| **Turn Windows feature on or off** and complete the following. | 1 Select **Internet Information Services** \| **FTP server** and select **FTP Extensibility**.<br>2 Select **Internet Information Services** \| **Web Management Tools** and select **IIS Management Service**.<br>3 Select **Telnet Server** and press OK.<br>This operation might take around 5 minutes to complete.<br>  |
| **Step 25:** Click **Start** and right-click **Computer**. Then select **Manage** \| **Services and Applications** \| **Services**. Then double-click **Telnet**. |  |

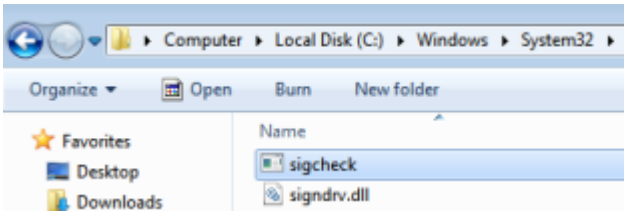
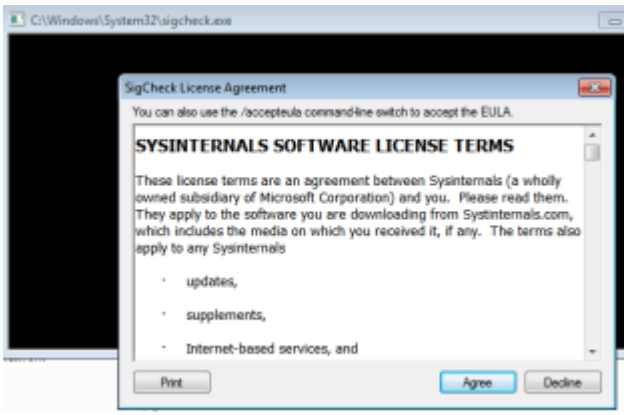
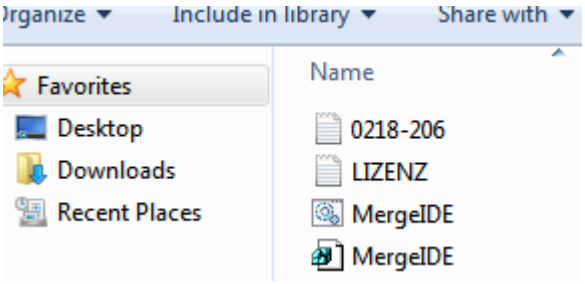
| Step | Details |
|---|---|
| Step 26: In the Telnet Properties (Local Computer) dialog, select **Automatic** from the **Startup type** list. Then select **Apply** \| **Start** \| **OK**. |  |

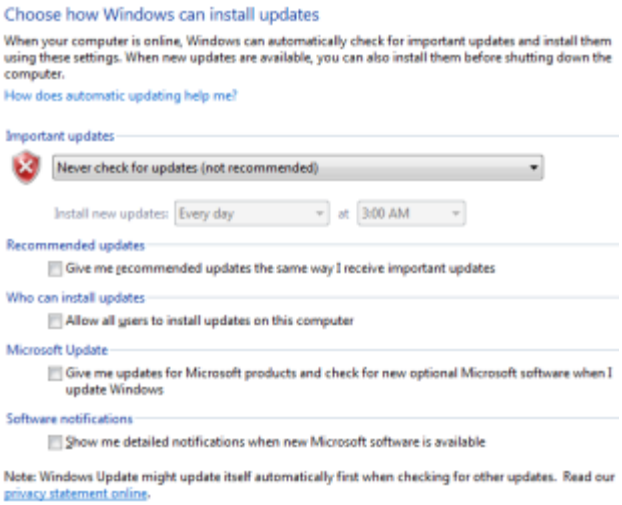
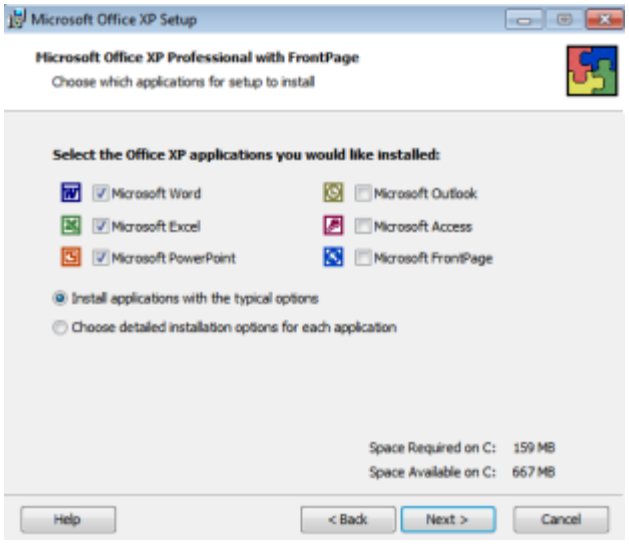
| Step | Details |
|---|---|
| **Step 27:** Enable FTP on the VM.<br>In the virtualMachineImage, select **Start** \| **Control Panel** \| **System and Security** \| **Administrative Tools**.<br>Double-click **Internet Information Services(IIS) Manager**, expand the tree under **Hostname**, and complete the following: | 1 Select **Sites** and right-click **Default Web Site** and remove. Confirm by clicking **Yes**.<br>  <br>2 Right-click **Sites** and select **Add FTP Site**. Then complete the following.<br>  <br>a For **FTP site name**, enter `root`.<br>b **Physical Path: C:\.** |

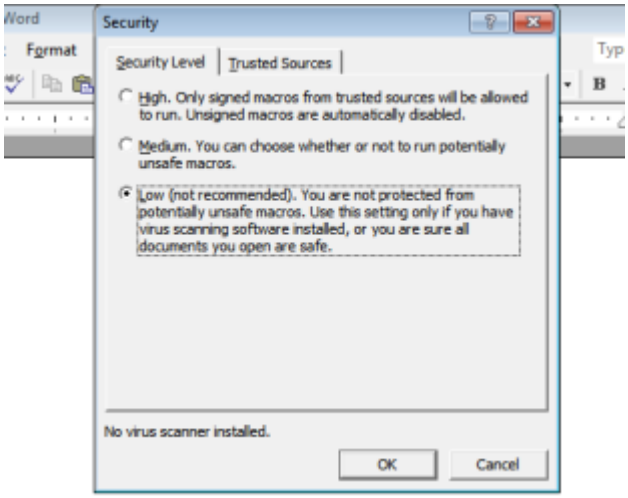
| Step | Details |
|---|---|
| | **c** Click **Next**.<br>  <br><br>3 For **Bindings and SSL Settings**, select **No SSL**. For all other fields, leave the default values and click **Next**.<br>  <br><br>**Figure 5-1 Binding and SSL settings**<br>4 For **Authentication and Authorization Information** complete the following.<br>**a** Select **Basic**.<br>**b** For **Allow access to**, select **All Users**.<br>**c** For **Permissions**, select both **Read** and **Write**, and then click **Finish**. |

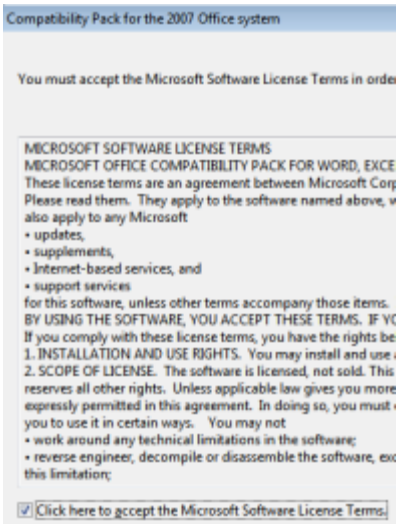
| Step | Details |
|---|---|
| | d Close the **Internet Information Services (IIS) Manager.**<br>  |
| **Step 28:** select **Start** \| **Run**, enter `netplwiz` and press **OK**. |  |

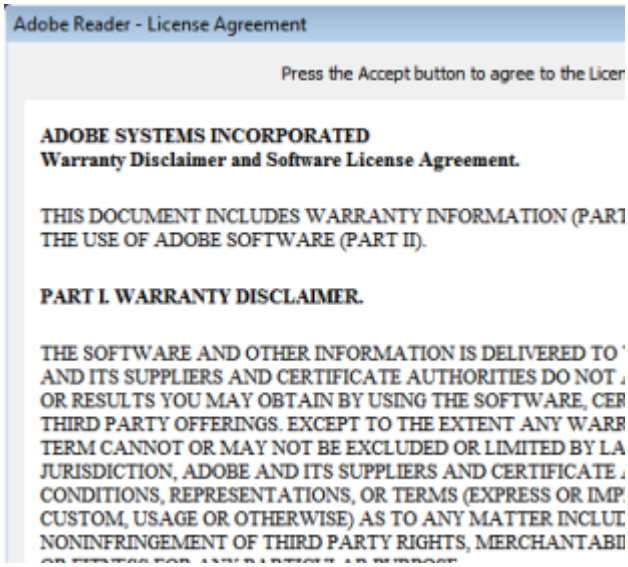
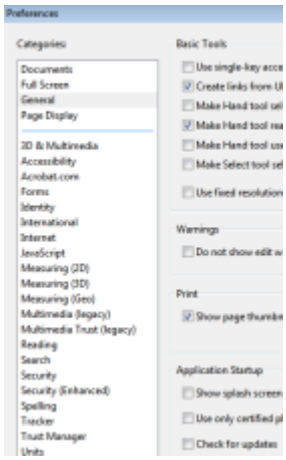
| Step | Details |
|---|---|
| **Step 29:** In the **User Accounts** window, deselect **Users must enter a user name and password to use this computer** and click **Apply**. |  |
| **Step 30:** In the **Automatically Log On** pop-up window, complete the following and then press **OK** in the message boxes. | • **User name** — Enter `Administrator`<br>• **Password** — Enter `cr@cker42`<br>• **Confirm Password** — Enter `cr@cker42`<br>  |
| **Step 31:** Download Sigcheck on to your computer (the native host) from http://technet.microsoft.com/en-us/sysinternals/bb897441.aspx. | The VM that you created has the Windows Firewall switch off as well as there is no anti-virus installed on it. Therefore, it is recommended that you download the programs and components on to the native host first and then copy them to the VM in VMware Workstation. |
| **Step 32:** Extract sigcheck.zip to `C:\WINDOWS\system32` location. | |

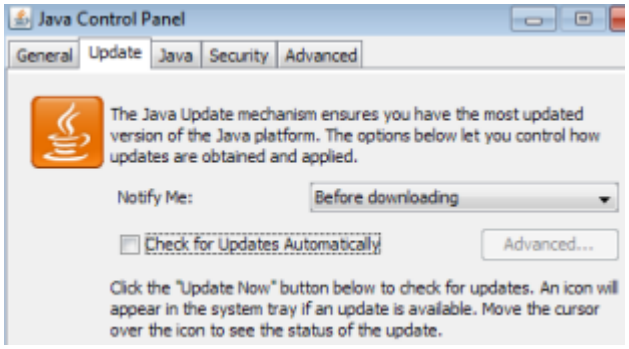
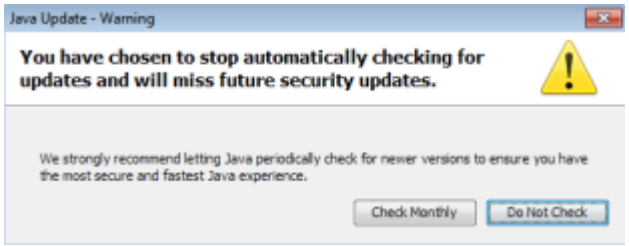
| Step | Details |
|---|---|
| **Step 33:** In Windows Explorer, go to C:\WINDOWS\system32 and double-click **sigcheck.exe**. |  |
| **Step 34** Click **Agree** for **Sigcheck License Agreement**.<br>After you click on **Agree**, no confirmation message is displayed. |  |
| **Step 35:** Download MergeIDE.zip from https://www.virtualbox.org/attachment/wiki/Migrate_Windows/MergeIDE.zip on to the native computer and then copy it to the VM. |  |
| **Step 36:** Extract MergeIDE.zip and run the MergeIDE batch file in the VM. | • If prompted, select **Run** in the warning message.<br>• Close Windows Explorer. |

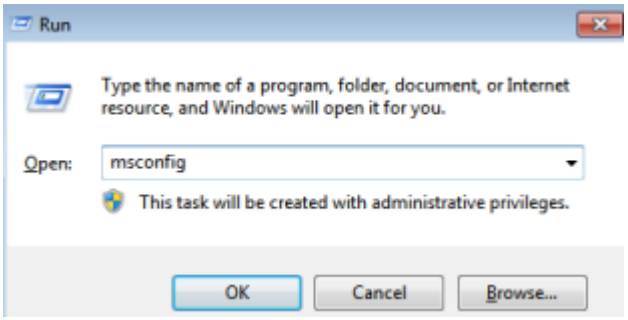
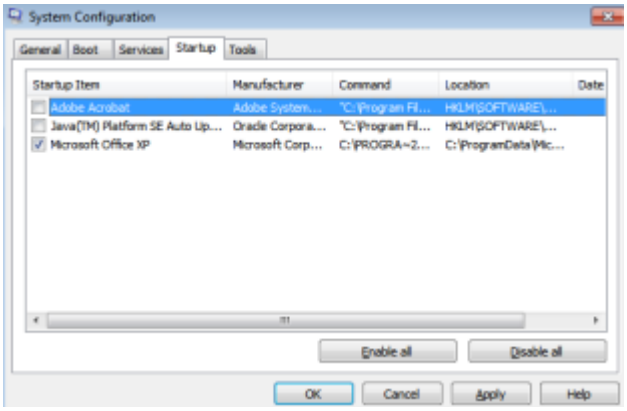
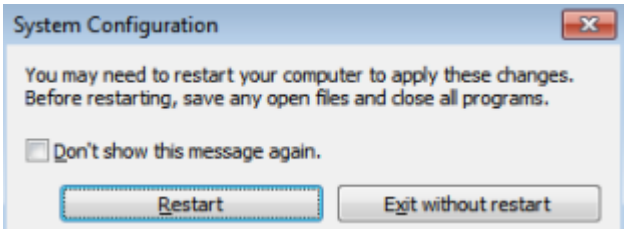
| Step | Details |
|---|---|
| **Step 37:** Disable Windows updates. | 1 Select **Start** \| **Control Panel** \| **Windows Update** \| **Change settings**.<br>2 In the **Change settings** page, complete the following.<br>a In the **Important updates** select **Never check for updates (not recommended)**.<br>b Deselect the check boxes under **Recommended updates, Who can install updates, Microsoft update, Software notifications.**<br>  <br>3 Click **OK**. |
| **Step 38:** To analyze Microsoft Word, Excel, and Powerpoint files, install Microsoft Office 2003 on the virtual machine. |  |

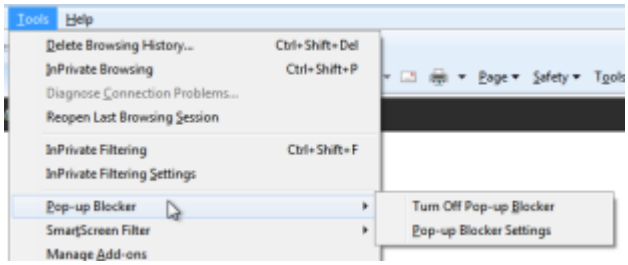
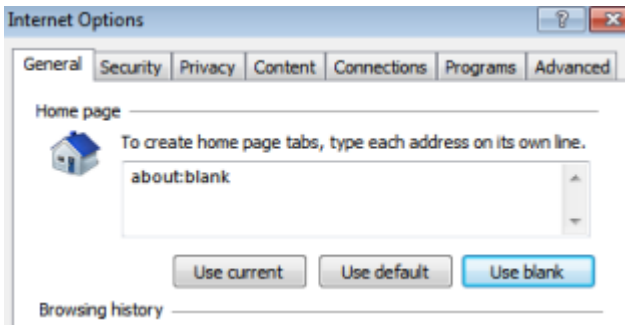
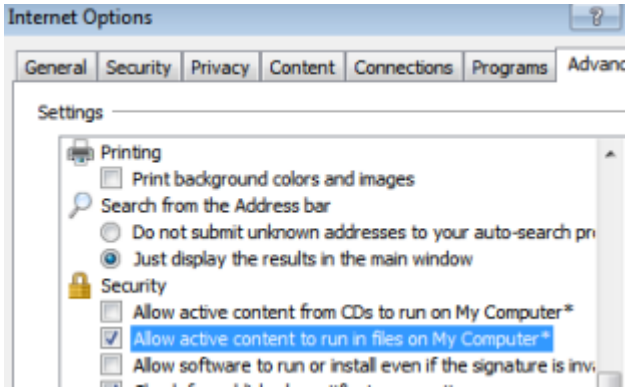
| Step | Details |
|---|---|
| **Step 39:** Lower the security to run macros for the Office applications. | • Open Microsoft Word 2003 and select **Tools** \| **Macro** \| **Security** and then select **Low** and click **OK**.<br>  <br>• Similarly lower the macro security for Microsoft Excel and Powerpoint. |
| **Step 40:** You need the compatibility pack to open Microsoft Office files that were created in a newer version of Microsoft Office. For example, to open a .docx file using Office 2003, you need the corresponding compatibility pack installed.<br>Go to http://www.microsoft.com/en-us/download/details.aspx?id=3 and download the required Microsoft Office compatibility pack for Word, Excel, and PowerPoint File Formats. Then install them on the virtual machine.<br>After you download the compatibility pack, install it on the virtual machine. To open files created by a later version of Microsoft Office applications, you must install the , | |

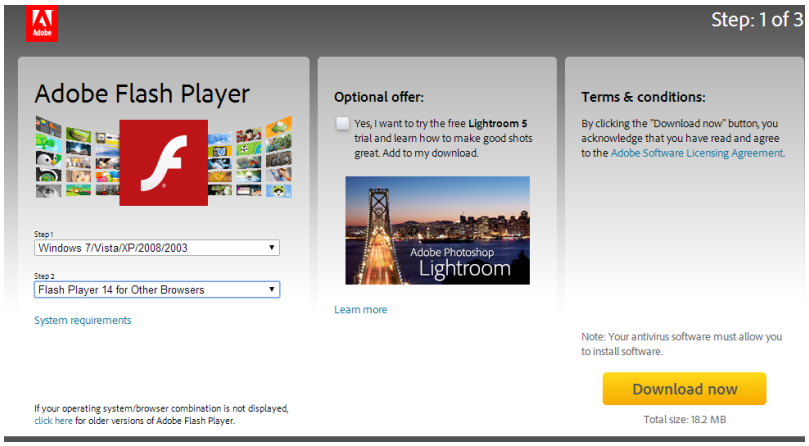
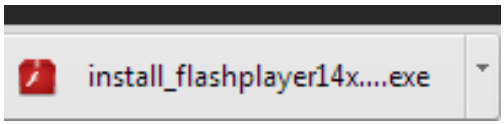
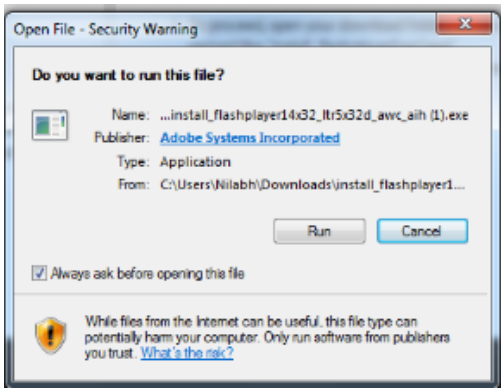
| Step | Details |
|---|---|
| **Step 41:** In the **Compatibility Pack for the 2007 Office system** dialog, select **Click here to accept the Microsoft Software License Terms** and click **Continue.** |  |

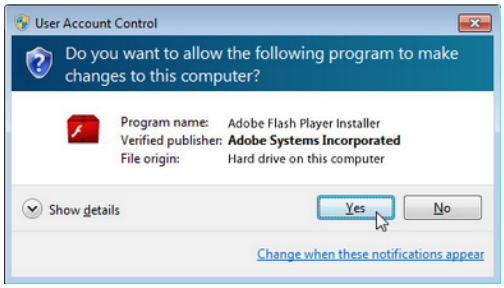
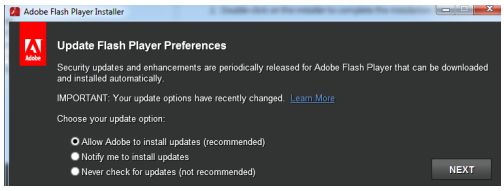
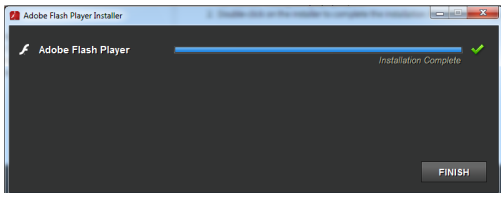
| Step | Details |
|---|---|
| **Step 42:** To analyze PDF files, download Adobe Reader to the native host and copy it to the VM.<br><br>This procedure uses Adobe Reader 9.0 as an example. | 1 Install Adobe Reader 9.0 in the VM.<br><br>2 Open Adobe Reader and click **Accept**.<br><br>  <br><br><br>3 In Adobe Reader, select **Edit** \| **Preferences** \| **General** and deselect **Check for updates**.<br><br>  <br> |

| Step | Details |
|---|---|
| **Step 43:** To analyze JAR files, download and install Java Runtime Environment.<br><br>This procedure uses Java 7 Update 25 as an example. | |
| **Step 44:** Open Java in Control Panel. | |
| **Step 45:**In the **Update** tab, deselect **Check for Updates Automatically.** |  |
| **Step 46:** In the Java Update Warning dialog, select **Do Not Check** and then click **OK** in the Java Control Panel. |  |

| Step | Details |
|---|---|
| **Step 47:** In the Windows Run dialog, enter `msconfig`. |  |
| **Step 48:** In the System Configuration utility, go to the **Startup** tab. |  <br>Deselect *reader_sl* and *jusched* and then click **OK**. |
| **Step 49:**: In the **System Configuration** dialog, click **Restart**. |  |

| Step | Details |
|---|---|
| **Step 50:** Open the default browser and set it up for malware analysis.<br><br>This procedure uses Internet Explorer as an example. | 1 Make sure the pop-up blocker is turned on. In Internet Explorer, select **Tools** \| **Pop-up Blocker** \| **Turn on Pop-up Blocker.**<br><br>  <br><br><br>2 Select **Tools** \| **Internet Options** and for **Home page** select **Use Blank** or **Use new tab** based on the version of Internet Explorer.<br><br>  <br><br><br>3 Go to the **Advanced** tab of the Internet Options and locate **Security.**<br><br>4 Select **Allow active content to run in files on My Computer.**<br><br>  <br><br><br>5 Click **OK.** |

| Step | Details |
|---|---|
| **Step 51:** To dynamically analyze Flash files (SWF), install the required version of Adobe Flash.<br><br>This procedure uses Flash Player 14 as an example. | 1 Goto http://get.adobe.com/flashplayer/otherversions/.<br><br>2 Select Operating System and Flash Player version respectively as per your requirement in **Step 1** and **Step 2** drop-down as shown below.<br><br>3 Click on **Download now** tab.<br><br>  <br><br>4 Double-click the Adobe Flash Player Installer file **(install_flashplayer xxx.exe)**, present at the bottom corner of your screen.<br><br>  <br><br>5 In the**Security Warning dialogue box**, Click **Run**.<br><br>  <br><br>6 In the **User Account Control** dialogue box, Click **Yes**. |

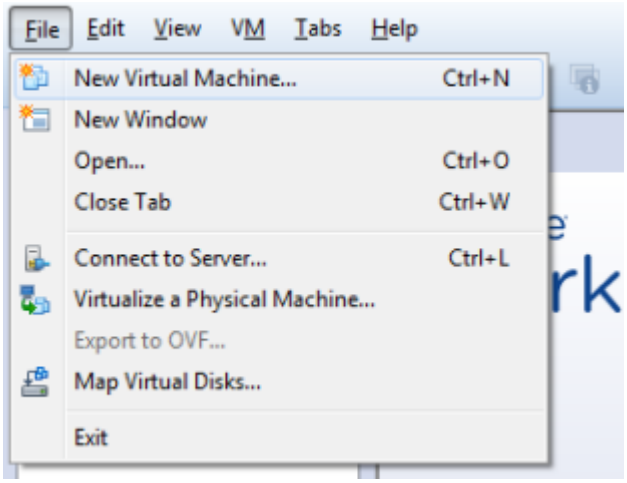
| Step | Details |
|---|---|
| |  <br>7 Choose your update option and Click **NEXT**.<br>  <br>8 Click **FINISH** to complete Adobe Flash Player installation.<br>  |
| **Step 52:** Shut down virtualMachineImage by selecting **Start** \| **Shut down.** | |
| **Step 53:** Go to the location that you provided in step 8 to find the VMDK file named as `virtualMachineImage-flat.vmdk` | |

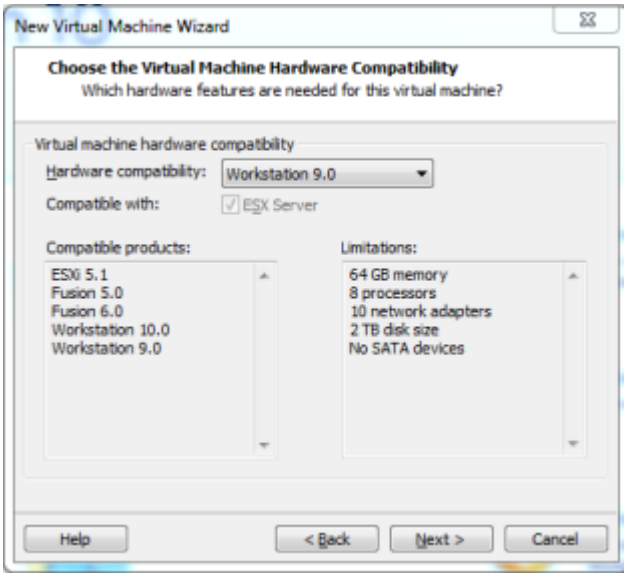
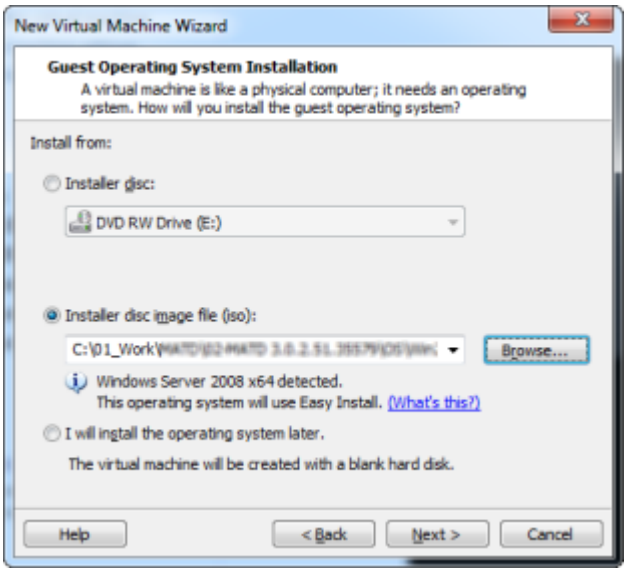
# Create a VMDK file for Windows 2008 Server

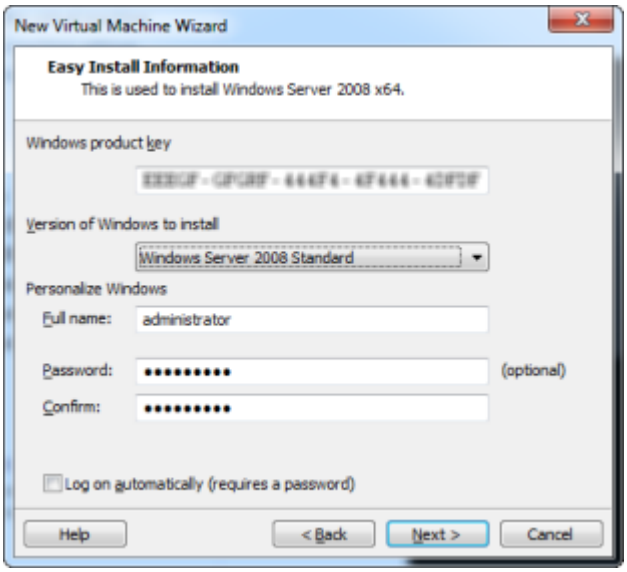
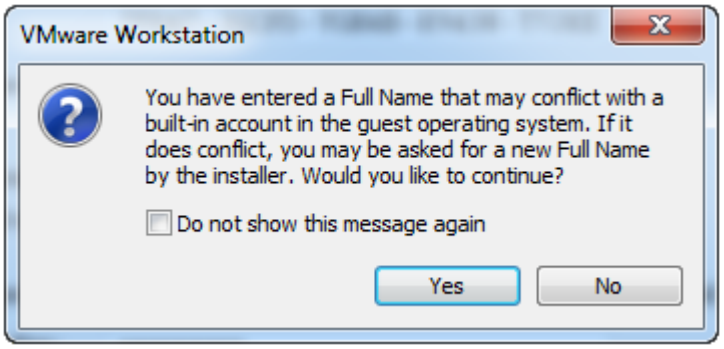
**Before you begin**

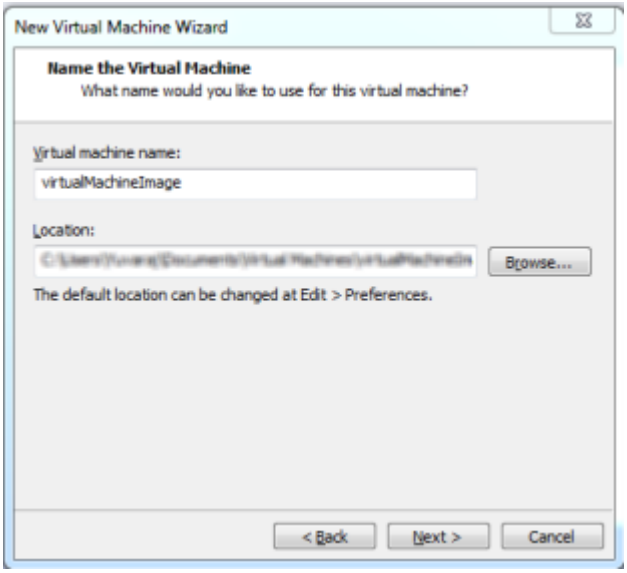
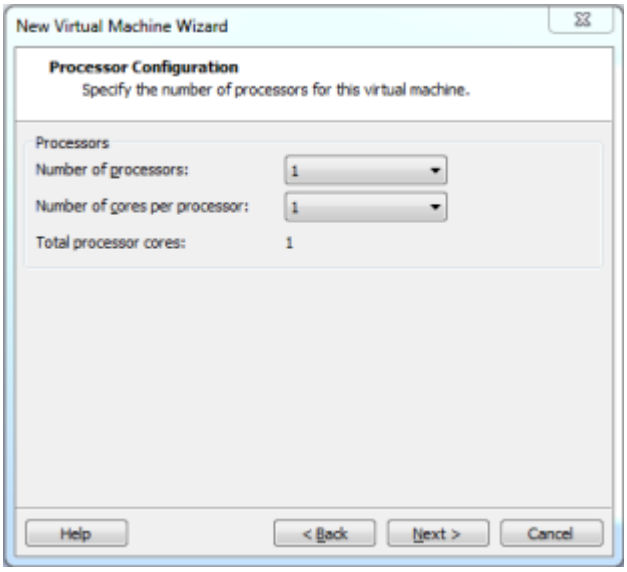
- Download VMware Workstation 9.0 or above from http://www.vmware.com/products/workstation/workstation-evaluation and install it.
- Make sure you have the ISO image of the operating system whose VMDK file you need to create.
- Make sure you have the license key for the operating system.

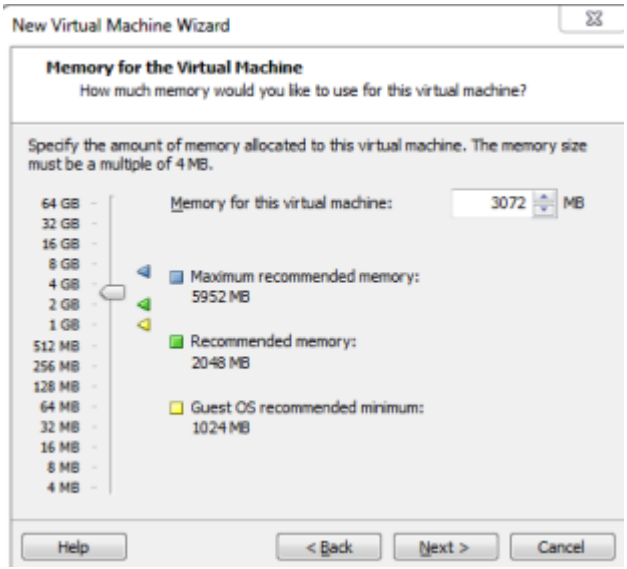
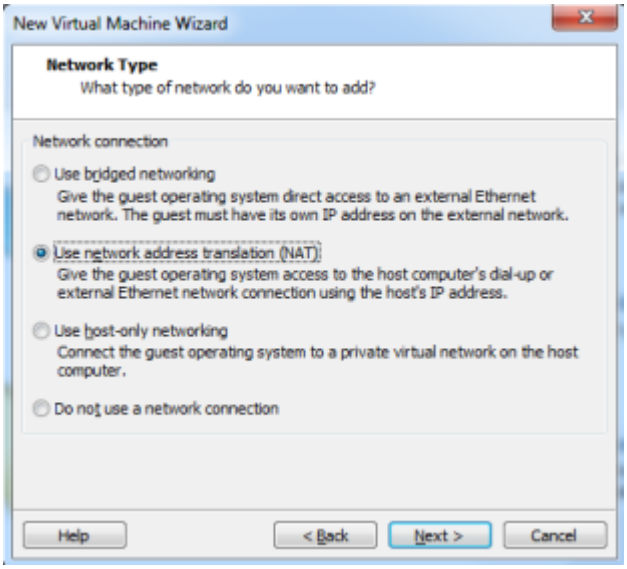
Use this procedure to create VMDK files from ISO images of Windows 2008 R2 SP1.

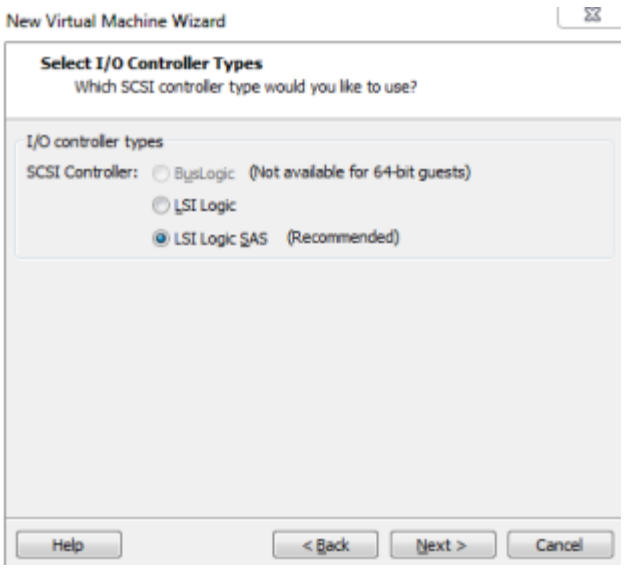
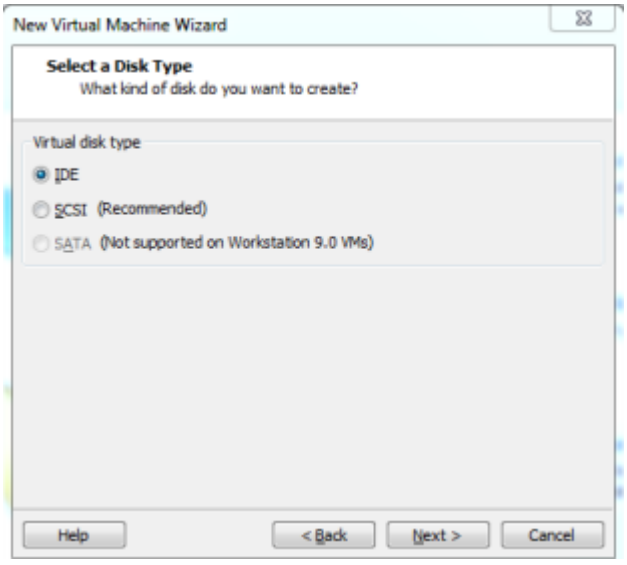
| Step | Details |
|---|---|
| **Step 1:** Start the VMware Workstation. | This procedure uses VMware Workstation 10 as an example. |
| **Step 2:** In the VMware Workstation page, select **File \| New Virtual Machine**. |  |
| **Step 3:** In the **New Virtual Machine Wizard** window, select **Custom (Advanced)** and click **Next**. | |

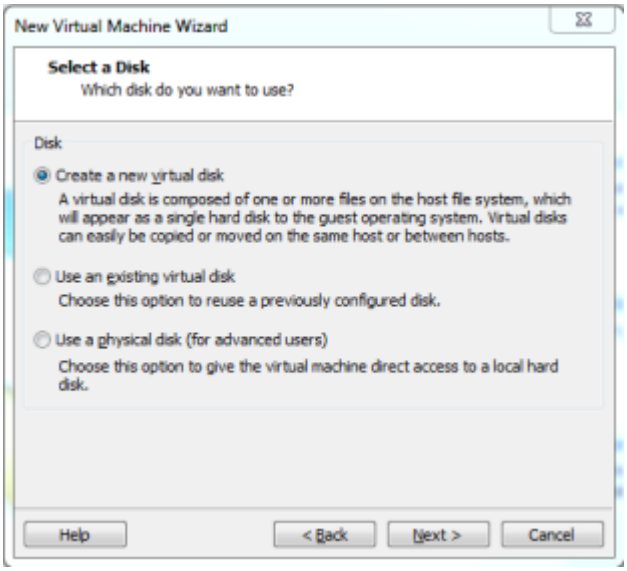
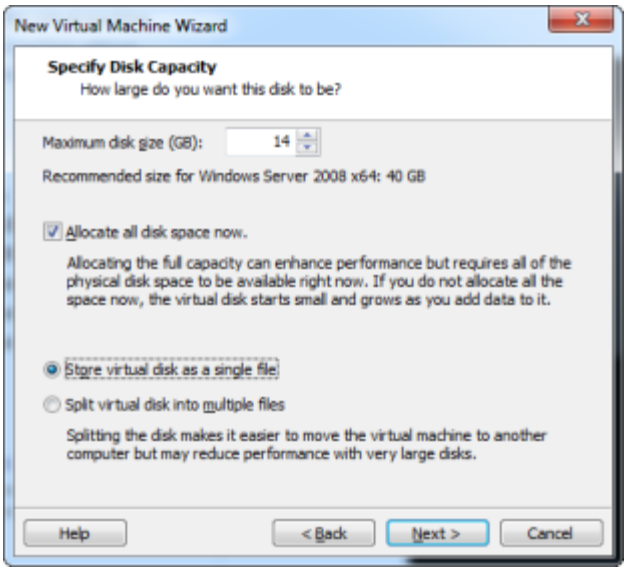
| Step | Details |
|---|---|
| **Step 4:** In the **Choose the Virtual Machine Hardware Compatibility** window, select **Workstation 9.0** from the **Hardware compatibility** drop-down list. For other fields, leave the default values and click **Next**. |  |
| **Step 5:** In the **Guest Operating System Installation** window, select either **Installer disc** or **Installer disc image file (iso)**, browse and select the ISO image, and then click **Next**. |  |

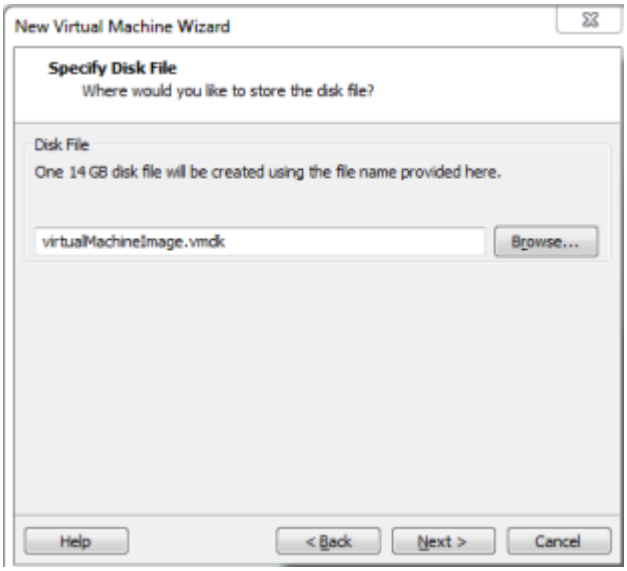
| Step | Details |
|---|---|
| **Step 6:** Enter the information in the **Easy Install Information** window and then click **Next**. | • **Windows product key** — Enter the license key of the Windows operating system for which you are creating the VMDK file.<br>• **Version of Windows to install** — Select the Standard or Enterprise version.<br>• **Full name** — You must enter `administrator` as the **Full name**.<br>• **Password** — You must enter `cr@cker42` as the password. This is the password that McAfee Advanced Threat Defense uses to log on to the VM.<br>• **Confirm** — Enter `cr@cker42` again to confirm.<br>• **Log on automatically (requires a password)** — Deselect this box.<br>  |
| **Step 7:** If the **VMware Workstation** message displays, click **Yes**. |  |

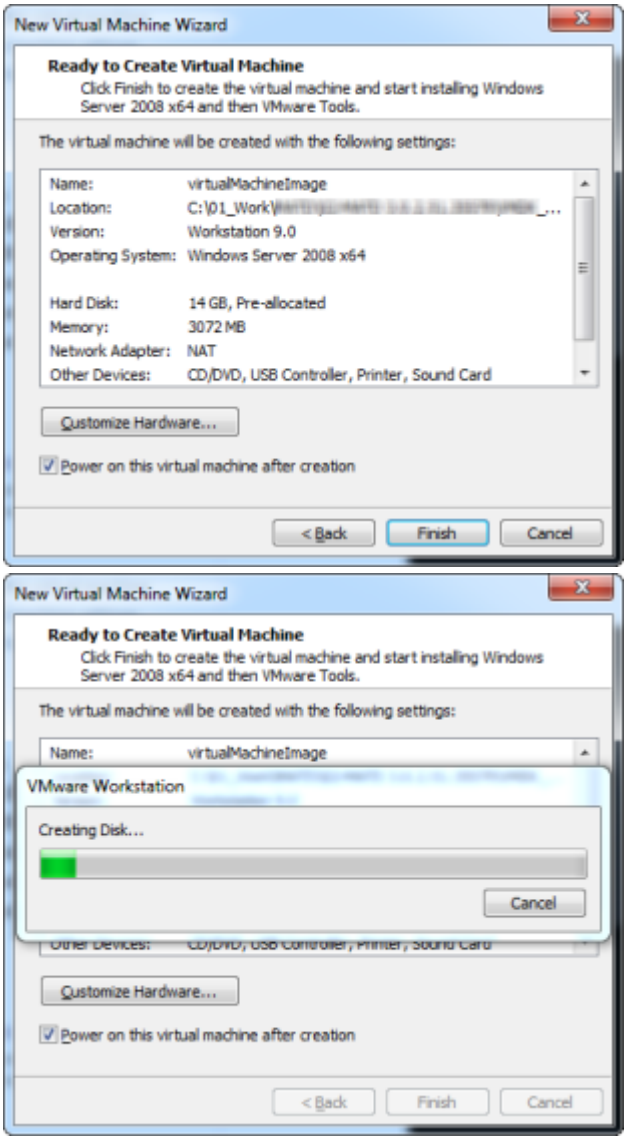
| Step | Details |
|---|---|
| **Step 8:** Enter the information in the **Name the Virtual Machine** window and then click **Next**. | • **Virtual Machine name** — You must enter `virtualMachineImage` as the name.<br>• **Location** — Browse and select the folder where you want to create the VMDK file.<br>  |
| **Step 9:** In the **Processor Configuration** window, leave the default values and click **Next**. |  |

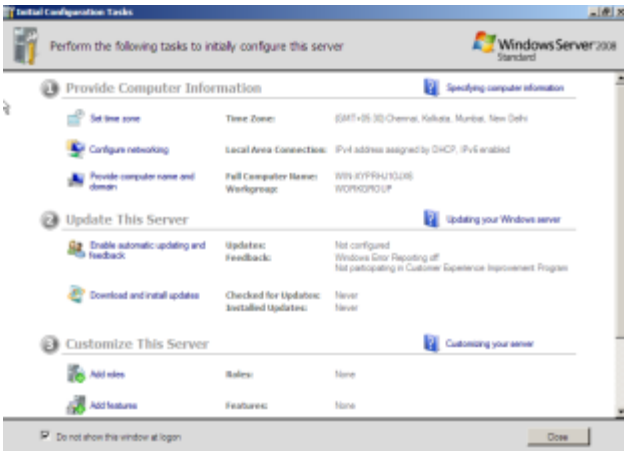
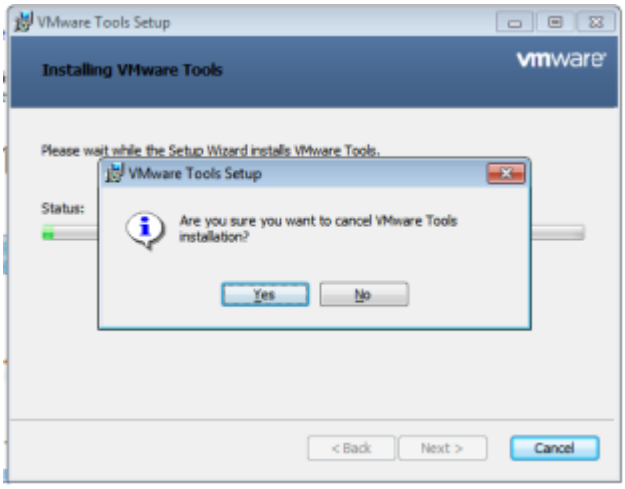
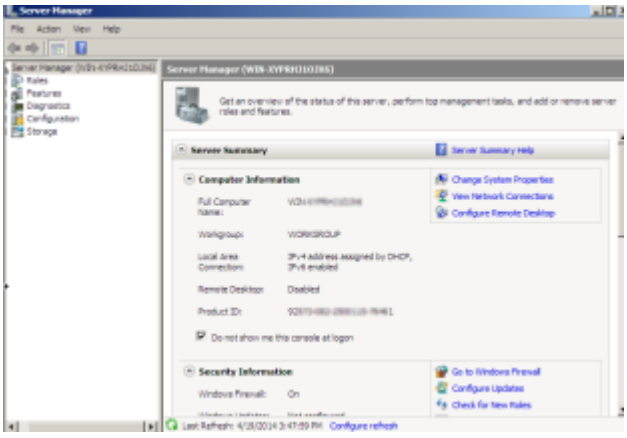
| Step | Details |
|---|---|
| **Step 10:** In the **Memory for the Virtual Machine** window, set 3072 MB as the memory. |  |
| **Step 11:** In the **Network Type** window, leave the default selection. |  |

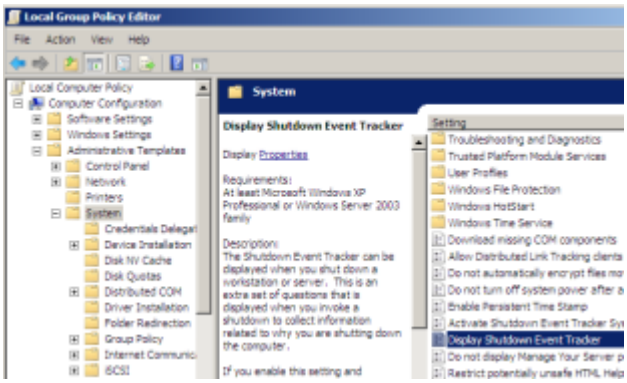
| Step | Details |
|---|---|
| **Step 12:** In the **Select I/O Controller Types** , leave the default selection. |  |
| **Step 13:** In the **Select a Disk Type** page, select **IDE** and click **Next**.<br><br>SCSI disks are not compatible with McAfee Advanced Threat Defense. |  |

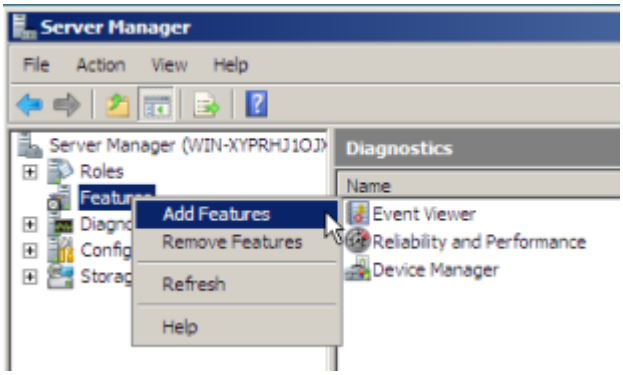
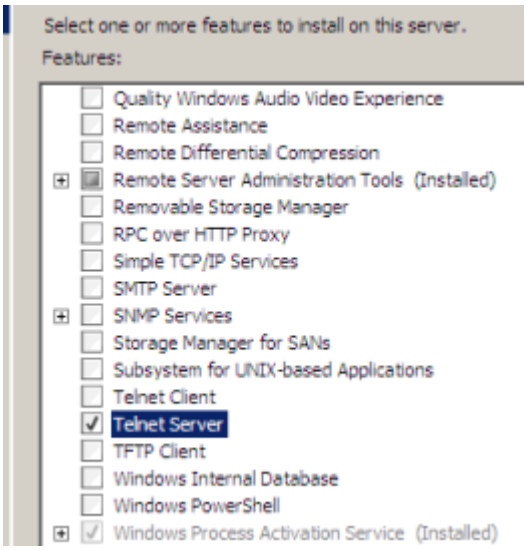
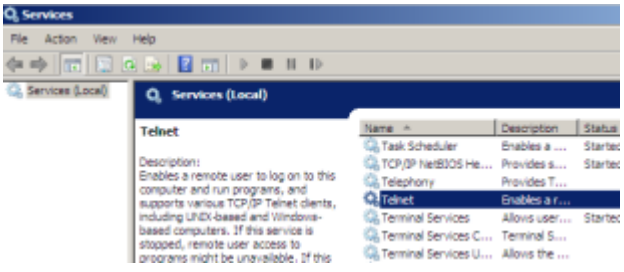
| Step | Details |
|---|---|
| **Step 14:** In the **Select a Disk** window, select **Create a new virtual disk** and click **Next**. |  |
| **Step 15:** Specify the details in the **Specify Disk Capacity** window and then click **Next**. | • **Maximum disk size (GB)** — You must enter 14 GB.<br>• Select **Allocate all disk space now.**<br>• Select **Store virtual disk as a single file.**<br>  |

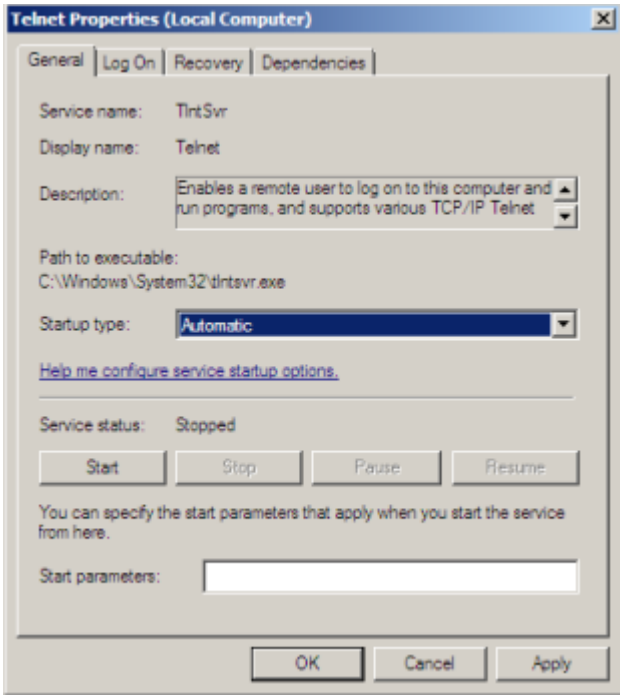
| Step | Details |
|---|---|
| **Step 16:** In the **Specify Disk file** window, make sure virtualMachineImage.vmdk is displayed by default and click **Next**.<br>If you specified a different name for **Virtual Machine name**, that name is displayed here. |  |

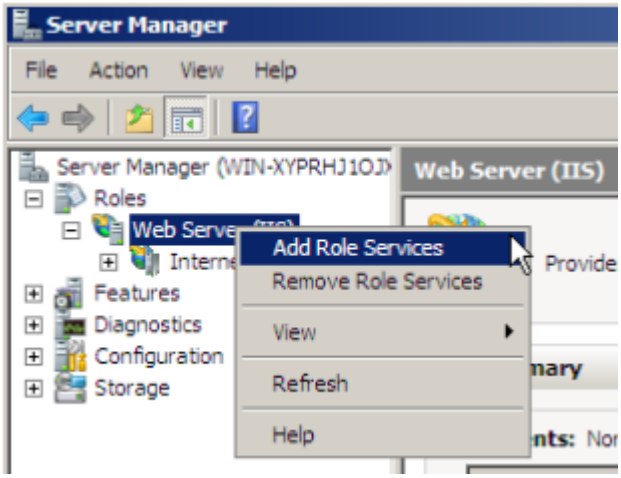
| Step | Details |
|---|---|
| **Step 17:** Complete the following in the **Ready to Create Virtual Machine** window. | • **Power on this virtual machine after creation** — Select this option.<br>• Click **Finish.**<br>This step might take around 30 minutes to complete.<br>  |
| **Step 18:** If the **Removable Devices** pop-up window is displayed, select **Do not show this hint again** and click **OK**. | Windows begins to install, which might take around 15 minutes. |

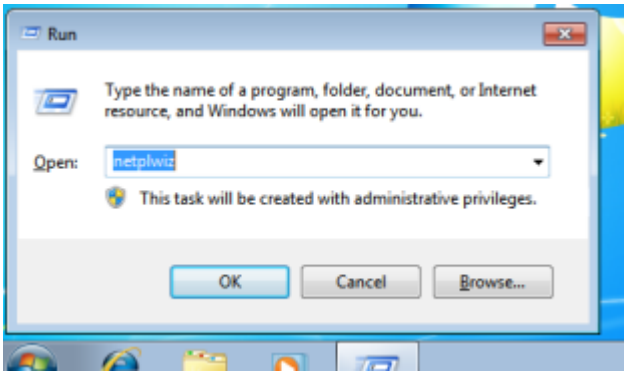
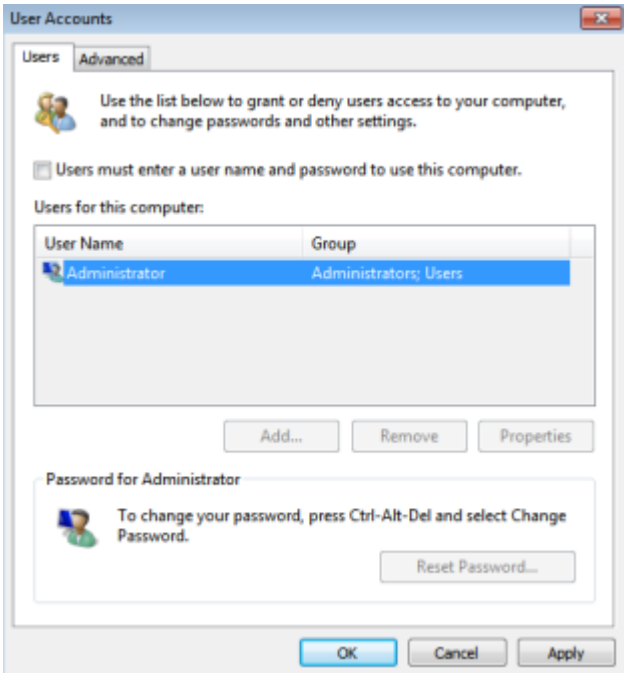
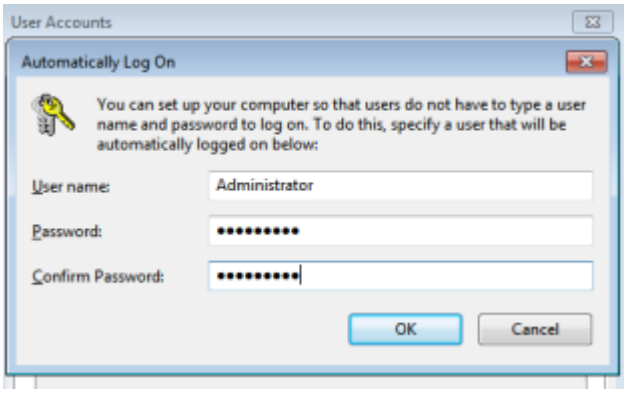
| Step | Details |
|---|---|
| **Step 19:** If the **Initial Configuration Tasks** window is displayed, select **Do not show this window at logon** and click **Close**. |  |
| **Step 20:** Stop the VMware Tools installation.<br>The VMware Tools are not compatible with McAfee Advanced Threat Defense. If you did not stop the VMware Tools installation, you can continue with the VMDK file creation process but make sure it is uninstalled when the VMDK file is ready. |  |
| **Step 21:** If the **Server Manager** window is displayed, select **Do not show me this console at logon** and close the window. |  |

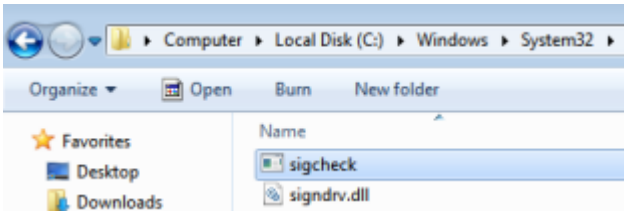
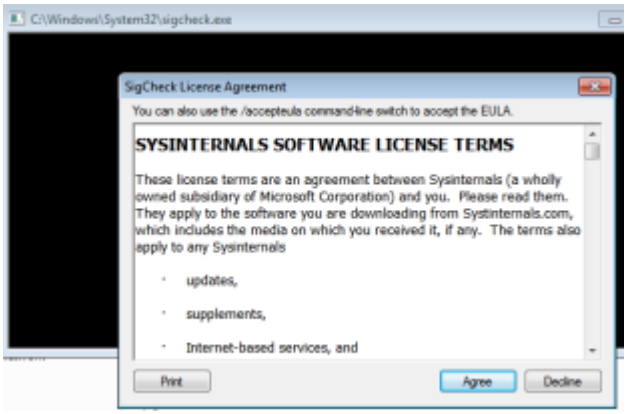
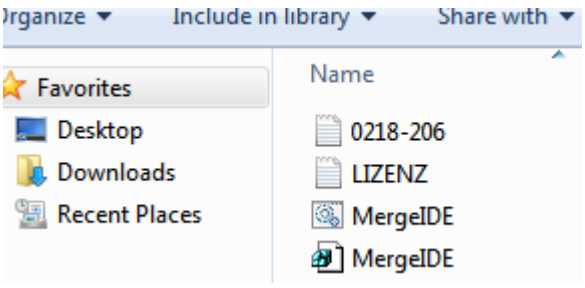
| Step | Details |
|---|---|
| **Step 22:** Complete the following. | 1 In the Windows Run window, enter `gpedit.msc` and press Enter.<br>2 In the **Local Group Policy Editor** window, select **Computer Configuration** \| **Administrative Templates** \| **System** and then double-click **Display Shutdown Event Tracker.**<br>  <br>3 In the **Display Shutdown Event Tracker Properties** dialog, select **Disabled** and click **OK.** |
| **Step 23:** In the VM, turn off the Windows Firewall. | 1 Select **Start** \| **Control Panel** \| **Windows Firewall** \| **Turn on Windows Firewall On or Off**<br>2 Select **Off** and then click **OK.** |

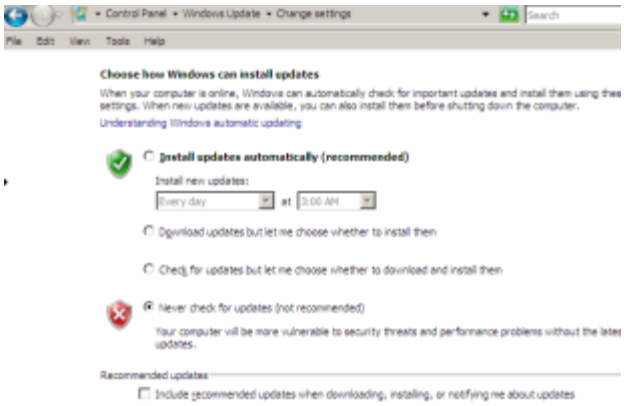
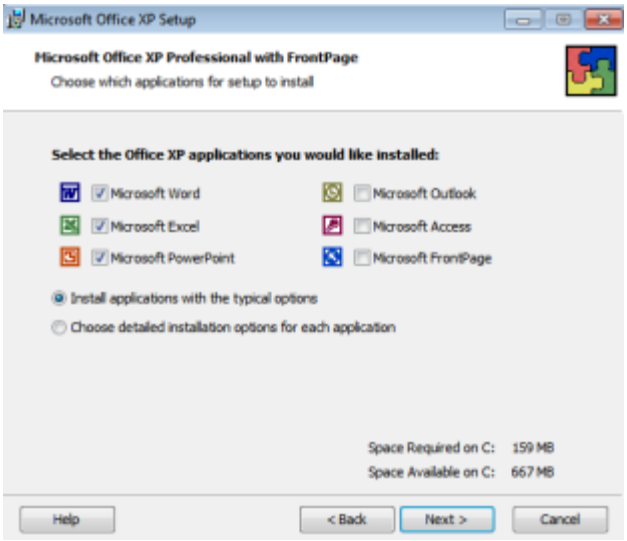
| Step | Details |
|---|---|
| **Step 24:** Enable the Telnet feature. | 1 In the virtualMachineImage, select **Start** \| **Administrative Tools** \| **Server Manager**.<br>2 In the **Server Manager** window, right-click **Features** and select **Add Features**.<br>  <br>3 In the **Add Features Wizard**, select **Telnet Server**.<br>  <br>4 Click **Next** and then **Install**.<br>5 Click **Close** after installation succeeds. |
| **Step 25:**Select **Start** \| **Administrative Tools** \| **Services**. Then double-click **Telnet**. |  |

| Step | Details |
|---|---|
| **Step 26**: In the Telnet Properties (Local Computer) dialog, select **Automatic** from the **Startup type** list. Then select **Apply** \| **Start** \| **OK**. |  |

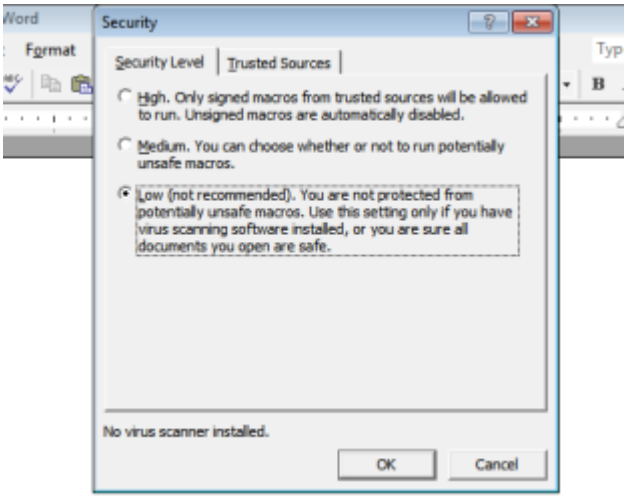
| Step | Details |
|---|---|
| **Step 27:** Enable FTP on the VM. | 1 In the virtualMachineImage, select **Start** \| **Administrative Tools** \| **Server Manager**.<br>2 In the **Server Manager** window select **Server Manager (virtual machine name)** \| **Roles** \| **Web Server (IIS)**.<br>3 Right-click on **Web Server (IIS)** and select **Add Role Services**.<br>  <br>4 In the **Add Role Services** wizard, select **FTP Publishing Service**.<br> <br>This installs the **FTP Server** and the **FTP Management Console**.<br>5 Click **Next** and then **Install**.<br>6 Click **Close** after the installation succeeds. |

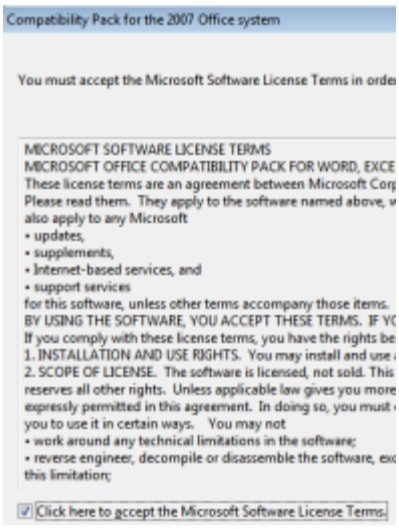
| Step | Details |
|---|---|
| **Step 28:** select **Start** \| **Run**, enter `netplwiz` and press **OK**. |  |
| **Step 29:** In the **User Accounts** window, deselect **Users must enter a user name and password to use this computer** and click **Apply**. |  |
| **Step 30:** In the **Automatically Log On** pop-up window, complete the following and then press **OK** in the message boxes. | • **User name** — Enter `Administrator`<br>• **Password** — Enter `cr@cker42`<br>• **Confirm Password** — Enter `cr@cker42`<br>  |

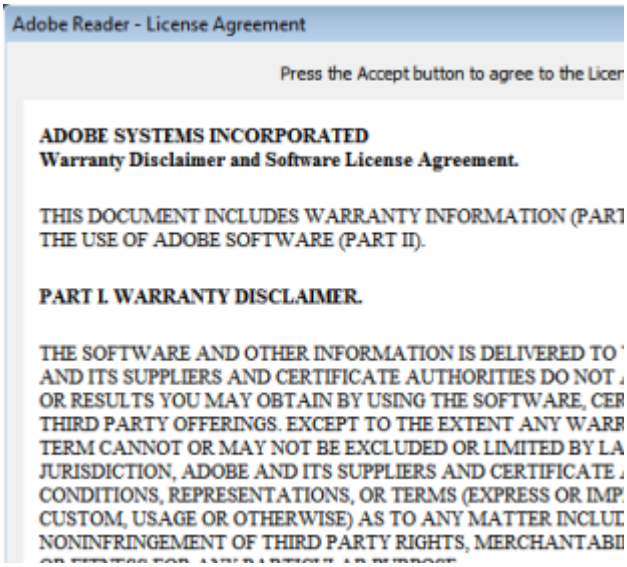
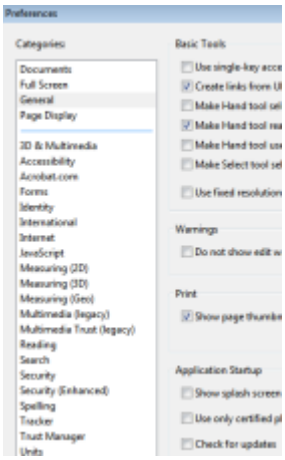
| Step | Details |
|---|---|
| **Step 31:** Download Sigcheck on to your computer (the native host) from http://technet.microsoft.com/en-us/sysinternals/bb897441.aspx. | The VM that you created has the Windows Firewall switch off as well as there is no anti-virus installed on it. Therefore, it is recommended that you download the programs and components on to the native host first and then copy them to the VM in VMware Workstation. |
| **Step 32:** Extract sigcheck.zip to `C:\WINDOWS\system32` location. | |
| **Step 33:** In Windows Explorer, go to C:\WINDOWS\system32 and double-click **sigcheck.exe**. |  |
| **Step 34** Click **Agree** for **Sigcheck License Agreement**.<br>After you click on **Agree**, no confirmation message is displayed. |  |
| **Step 35:** Download MergeIDE.zip from https://www.virtualbox.org/attachment/wiki/Migrate_Windows/MergeIDE.zip on to the native computer and then copy it to the VM. |  |
| **Step 36:** Extract MergeIDE.zip and run the MergeIDE batch file in the VM. | • If prompted, select **Run** in the warning message.<br>• Close Windows Explorer. |

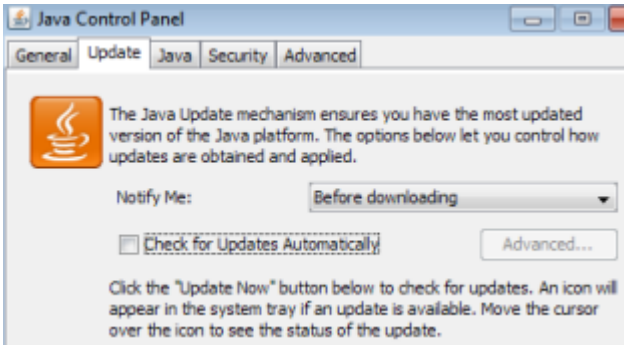
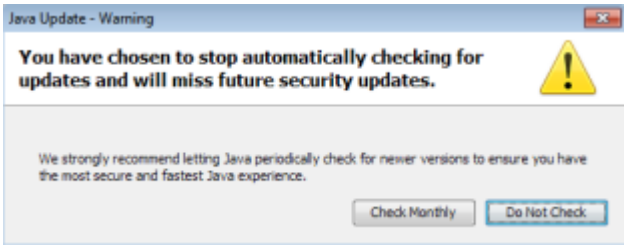
| Step | Details |
|---|---|
| **Step 37:** Disable Windows updates. | 1 Select **Start** \| **Control Panel** \| **Windows Update** \| **Change settings**.<br>2 In the **Change settings** page, complete the following.<br>a Select **Never check for updates (not recommended)**.<br>b Deselect the check box under **Recommended updates**.<br>  <br>3 Click **OK**. |
| **Step 38:** To analyze Microsoft Word, Excel, and Powerpoint files, install Microsoft Office 2003 on the virtual machine. |  |

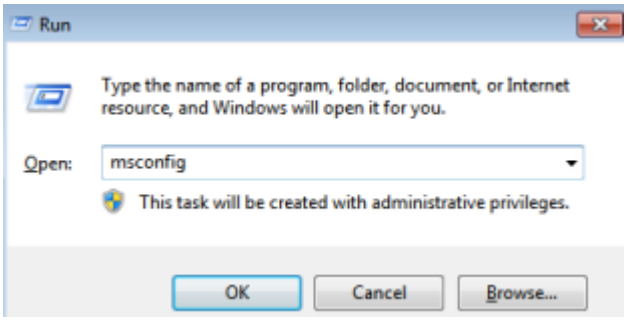
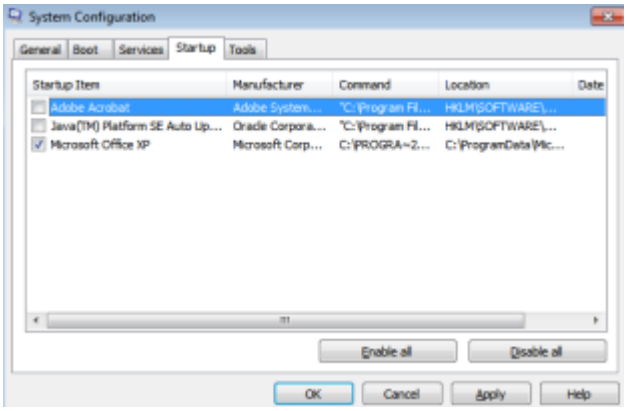
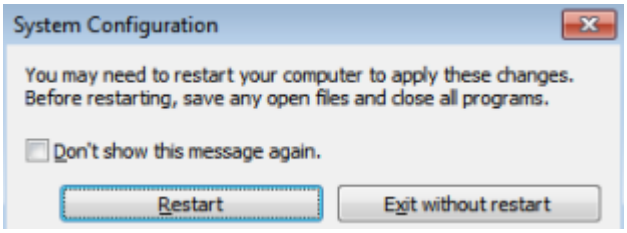
Microsoft Office XP Setup
Microsoft Office XP Professional with FrontPage
Choose which applications for setup to install
Select the Office XP applications you would like installed:
Microsoft Word
Microsoft Outlook
Microsoft Excel
Microsoft Access
Microsoft PowerPoint
Microsoft FrontPage
Install applications with the typical options
Choose detailed installation options for each application
Space Required on C: 159 MB
Space Available on C: 667 MB
Help
< Back
Next >
Cancel

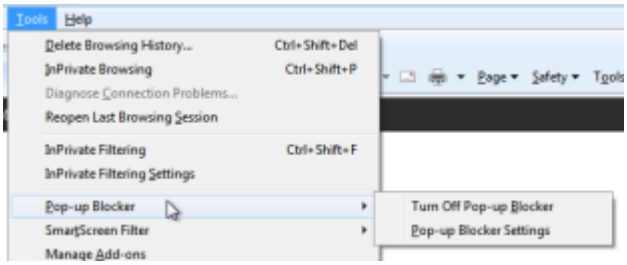
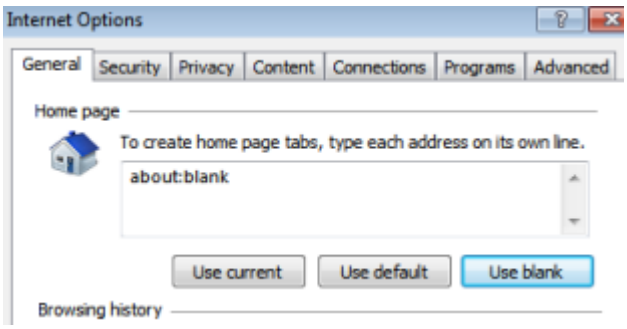
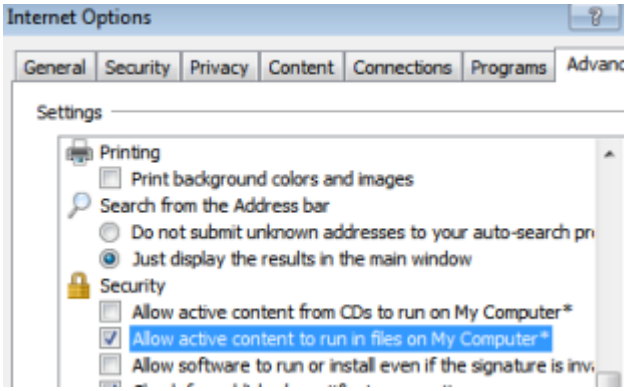
| Step | Details |
|---|---|
| **Step 39:** Lower the security to run macros for the Office applications. | • Open Microsoft Word 2003 and select **Tools** \| **Macro** \| **Security** and then select **Low** and click **OK**.<br>  <br>• Similarly lower the macro security for Microsoft Excel and Powerpoint. |
| **Step 40:** You need the compatibility pack to open Microsoft Office files that were created in a newer version of Microsoft Office. For example, to open a .docx file using Office 2003, you need the corresponding compatibility pack installed.<br>Go to http://www.microsoft.com/en-us/download/details.aspx?id=3 and download the required Microsoft Office compatibility pack for Word, Excel, and PowerPoint File Formats. Then install them on the virtual machine. | |

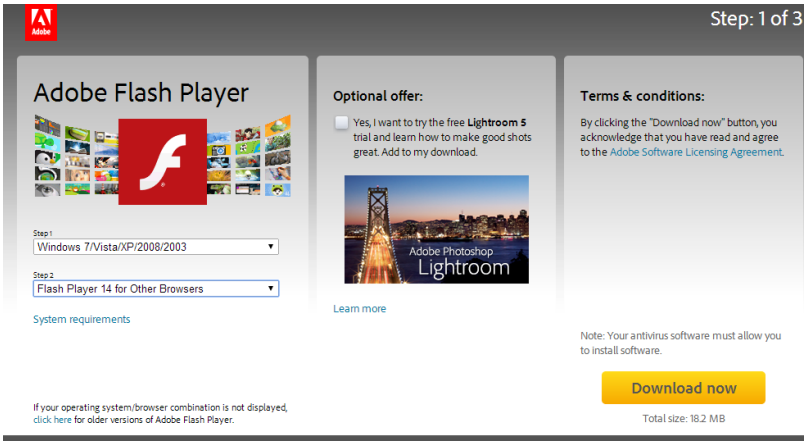
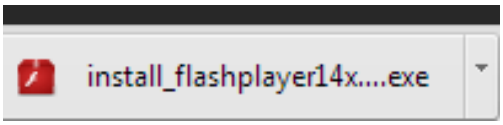
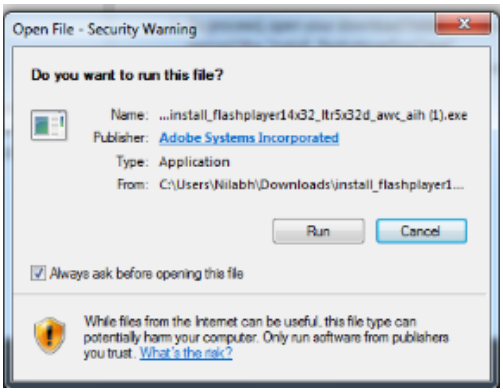
| Step | Details |
|---|---|
| **Step 41:** In the **Compatibility Pack for the 2007 Office system** dialog, select **Click here to accept the Microsoft Software License Terms** and click **Continue.** |  |

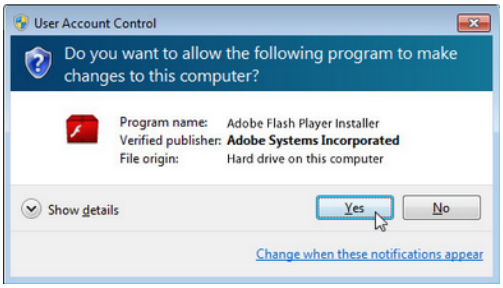
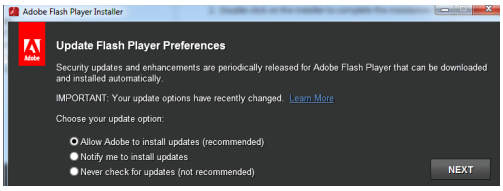
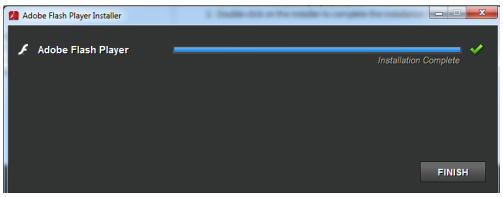
| Step | Details |
|---|---|
| **Step 42:** To analyze PDF files, download Adobe Reader to the native host and copy it to the VM.<br><br>This procedure uses Adobe Reader 9.0 as an example. | 1 Install Adobe Reader 9.0 in the VM.<br><br>2 Open Adobe Reader and click **Accept**.<br><br>  <br><br>3 In Adobe Reader, select **Edit** \| **Preferences** \| **General** and deselect **Check for updates**.<br><br>  |

| Step | Details |
|---|---|
| **Step 43:** To analyze JAR files, download and install Java Runtime Environment.<br><br>This procedure uses Java 7 Update 25 as an example. | |
| **Step 44:** Open Java in Control Panel. | |
| **Step 45:** In the **Update** tab, deselect **Check for Updates Automatically.** |  |
| **Step 46:** In the Java Update Warning dialog, select **Do Not Check** and then click **OK** in the Java Control Panel. |  |

| Step | Details |
|---|---|
| **Step 47:** In the Windows Run dialog, enter `msconfig`. |  |
| **Step 48:** In the System Configuration utility, go to the **Startup** tab. |  <br>Deselect all the items and click **OK**. |
| **Step 49:** In the **System Configuration** dialog, select **Don't show this message again** and click **Restart**. |  |

| Step | Details |
|---|---|
| **Step 50:** Open the default browser and set it up for malware analysis.<br><br>This procedure uses Internet Explorer as an example. | 1 Make sure the pop-up blocker is turned off. In Internet Explorer, select **Tools** \| **Pop-up Blocker** \| **Turn off Pop-up Blocker.**<br><br>  <br><br>2 Select **Tools** \| **Internet Options** and for **Home page** select **Use Blank** or **Use new tab** based on the version of Internet Explorer.<br><br>  <br><br>3 Go to the **Advanced** tab of the Internet Options and locate **Security.**<br><br>4 Select **Allow active content to run in files on My Computer.**<br><br>  <br><br>5 Click **OK.** |

| Step | Details |
|---|---|
| **Step 51:** To dynamically analyze Flash files (SWF), install the required version of Adobe Flash.<br><br>This procedure uses Flash Player 14 as an example. | 1 Goto http://get.adobe.com/flashplayer/otherversions/.<br><br>2 Select Operating System and Flash Player version respectively as per your requirement in **Step 1** and **Step 2** drop-down as shown below.<br><br>3 Click on **Download now** tab.<br><br>  <br><br>4 Double-click the Adobe Flash Player Installer file **(install_flashplayer xxx.exe)**, present at the bottom corner of your screen.<br><br>  <br><br>5 In the**Security Warning dialogue box**, Click **Run**.<br><br>  <br><br>6 In the **User Account Control** dialogue box, Click **Yes**. |

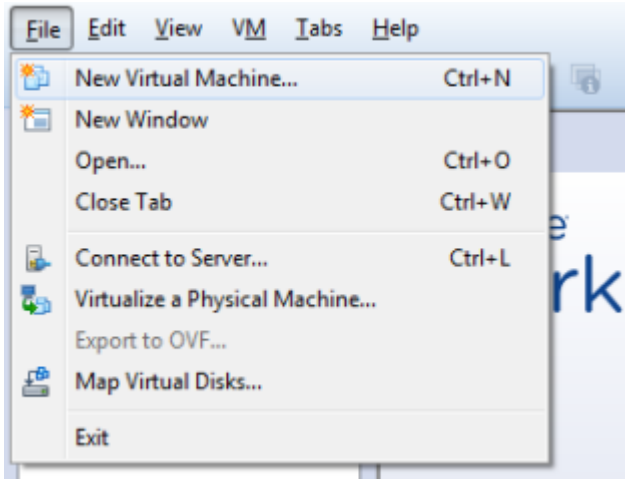
| Step | Details |
|---|---|
| |  <br>7 Choose your update option and Click **NEXT**.<br>  <br>8 Click **FINISH** to complete Adobe Flash Player installation.<br>  |
| **Step 52:** Shut down virtualMachineImage by selecting **Start** \| **Shut down.** | |
| **Step 53:** Go to the location that you provided in step 8 to find the VMDK file named as `virtualMachineImage-flat.vmdk` | |

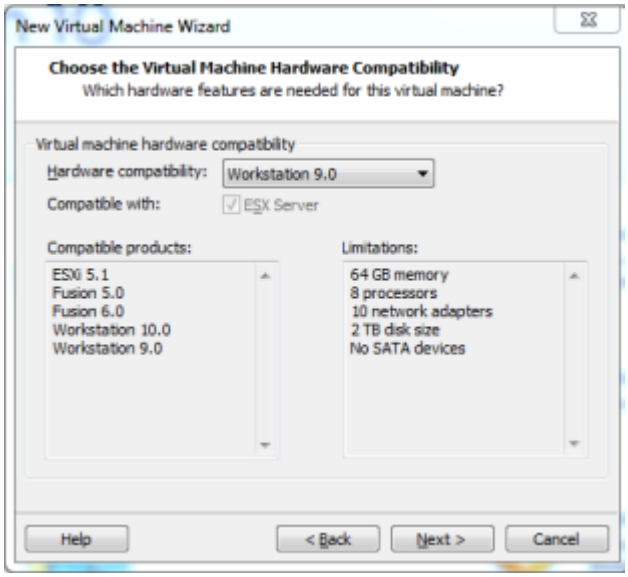
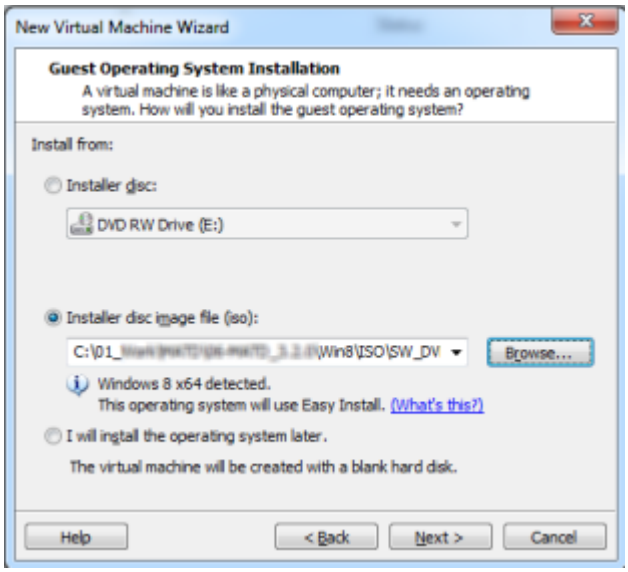
# Create a VMDK file for Windows 8

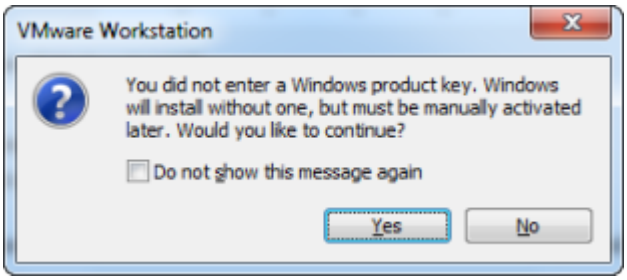
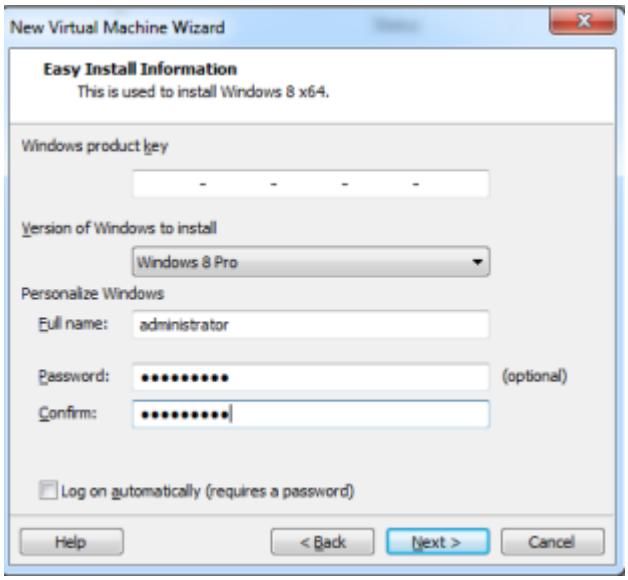
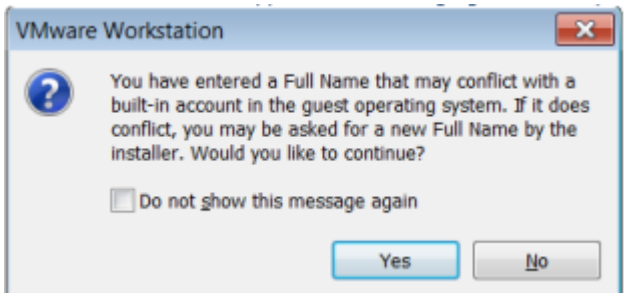
**Before you begin**

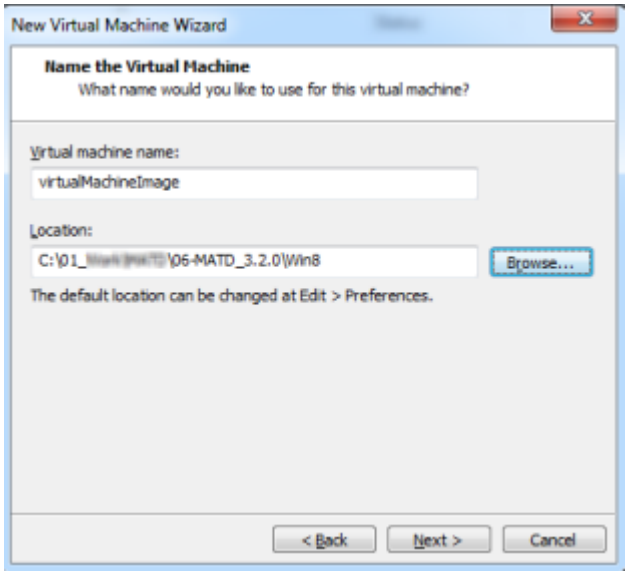
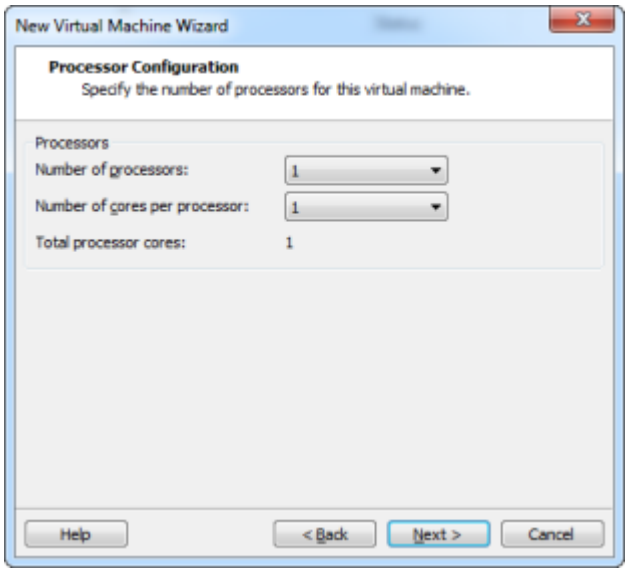
- Download VMware Workstation 9.0 or above from http://www.vmware.com/products/workstation/workstation-evaluation and install it. McAfee recommends version 9 or 10.
- Make sure that you have the ISO image of Windows 8 32-bit or 64-bit for which you need to create the VMDK file. Only Windows 8 Pro is supported. This procedure uses Windows 8 Pro English version as an example.
- Make sure you have the details to activate the operating system based on the type of license you possess. You must activate the operating system before you import the VMDK file into McAfee Advanced Threat Defense.

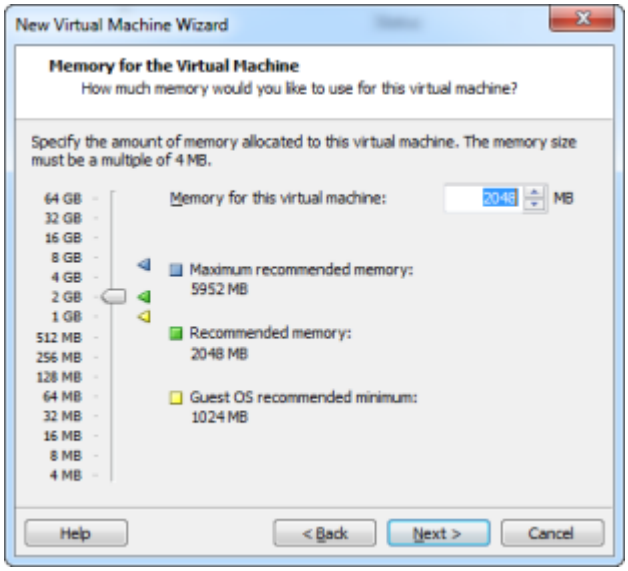
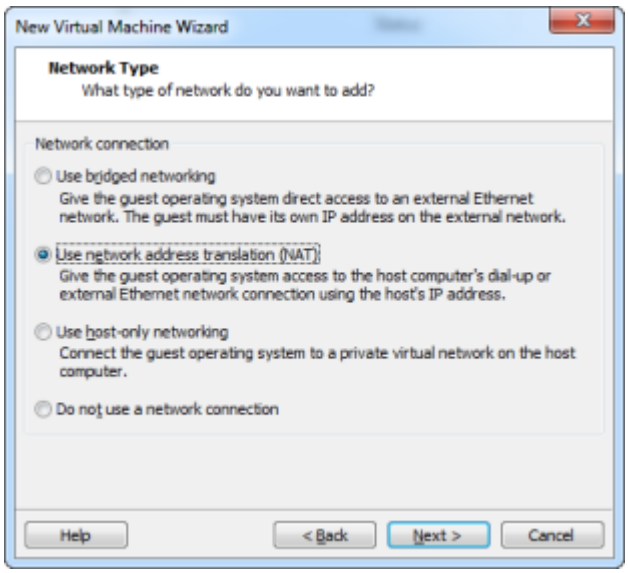
Use this procedure to create VMDK files from an ISO image of Windows 8 Pro 32 bit or 64 bit.

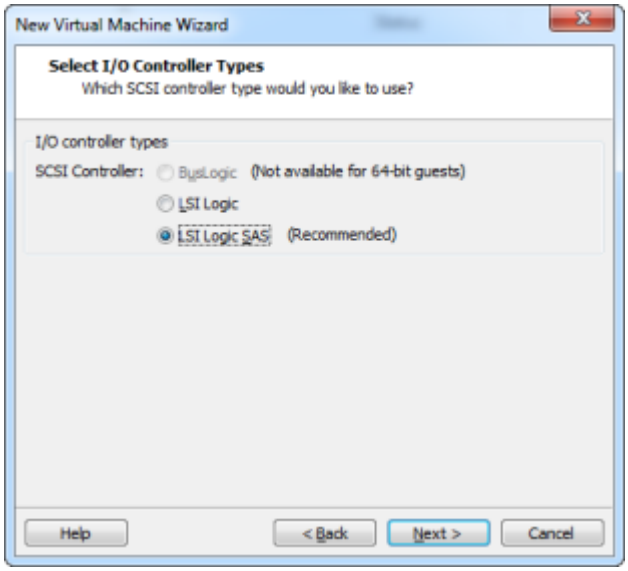
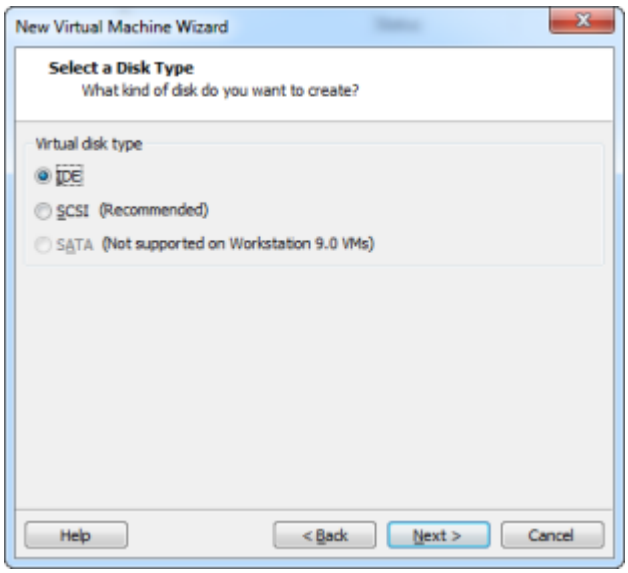
| Step | Details |
|---|---|
| **Step 1:** Start the VMware Workstation. | This procedure uses VMware Workstation 10 as an example. |
| **Step 2:** In the VMware Workstation page, select **File \| New Virtual Machine.** |  |
| **Step 3:** In the **New Virtual Machine Wizard** window, select **Custom (Advanced)** and click **Next.** | |

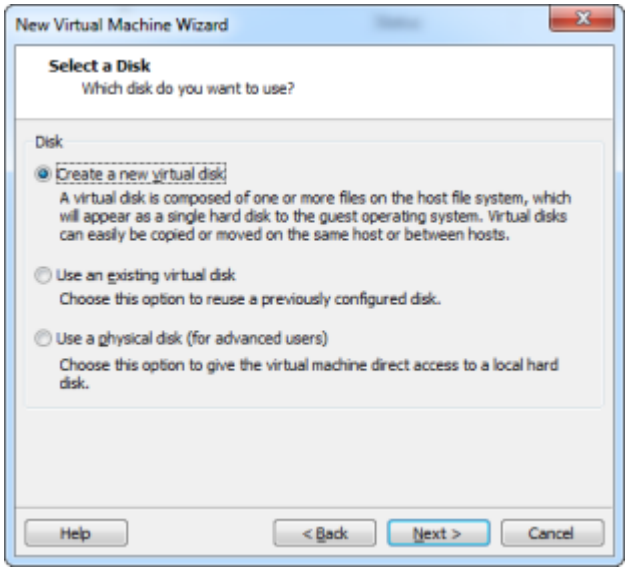
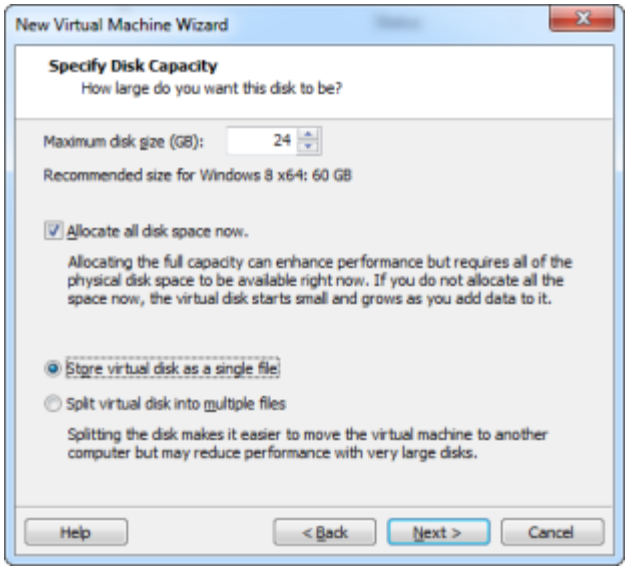
| Step | Details |
|---|---|
| **Step 4:** In the **Choose the Virtual Machine Hardware Compatibility** window, select **Workstation 9.0** from the **Hardware compatibility** drop-down list. For other fields, leave the default values and click **Next**. |  |
| **Step 5:** In the **Guest Operating System Installation** window, select **Installer disc image file (iso)**, browse and select the ISO image, and then click **Next**. |  |

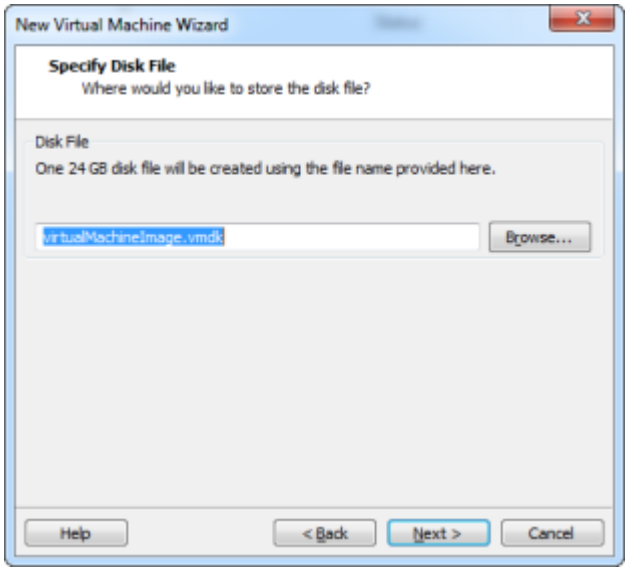
| Step | Details |
|---|---|
| **Step 6:** Enter the information in the **Easy Install Information** window and then click **Next**. | • **Windows product key** — Enter the license key of the Windows operating system for which you are creating the VMDK file. For volume license, you can leave it empty. Click **Yes** if the following message is displayed subsequently.<br>  <br>• **Full name** — Enter `administrator` as the **Full name**.<br>• **Password** — Enter `cr@cker42` as the password. McAfee Advanced Threat Defense uses this password to log on to the VM.<br>• **Confirm** — Enter `cr@cker42` again to confirm.<br>• **Log on automatically (requires a password)** — Deselect this box.<br>  |
| **Step 7:** If the **VMware Workstation** message displays, click **Yes**. |  |

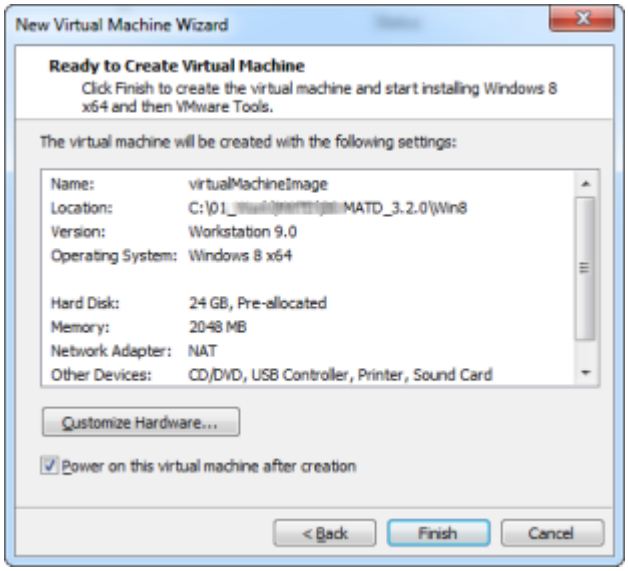
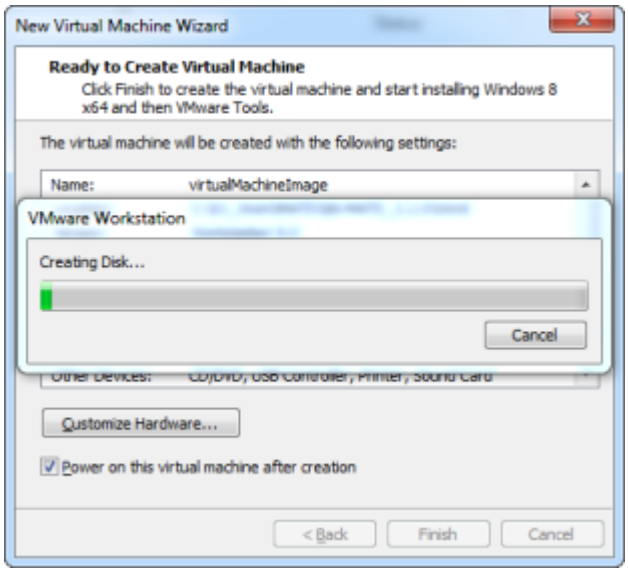
| Step | Details |
|---|---|
| **Step 8:** Enter the information in the **Name the Virtual Machine** window and then click **Next**. | • **Virtual Machine name** — You must enter `virtualMachineImage` as the name.<br>• **Location** — Browse and select the folder where you want to create the VMDK file.<br>  |
| **Step 9:** In the **Processor Configuration** window, leave the default values and click **Next**. |  |

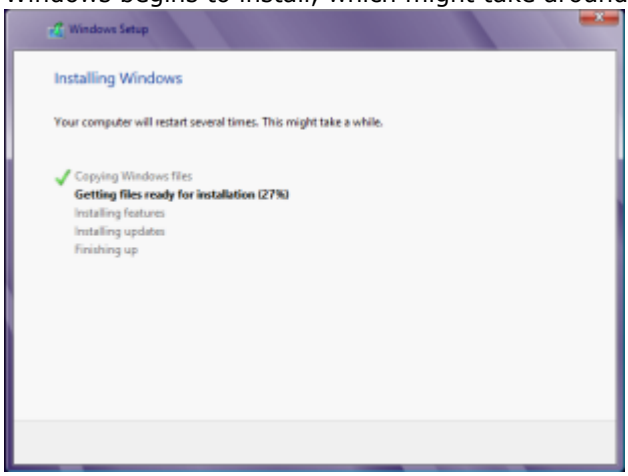
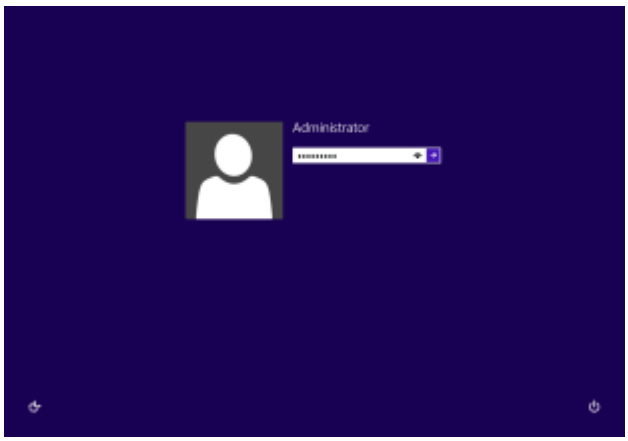
| Step | Details |
|---|---|
| **Step 10:** In the **Memory for the Virtual Machine** window, set 2048 MB as the memory. |  |
| **Step 11:** In the **Network Type** window, leave the default selection. |  |

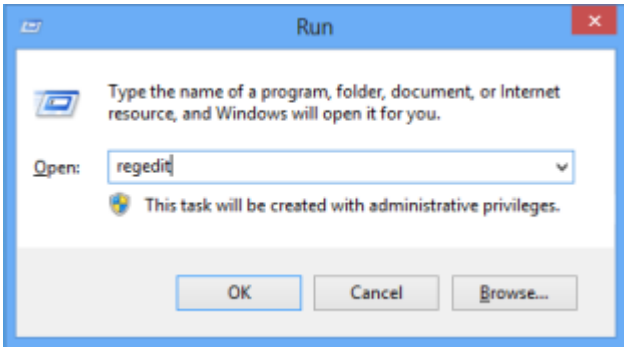
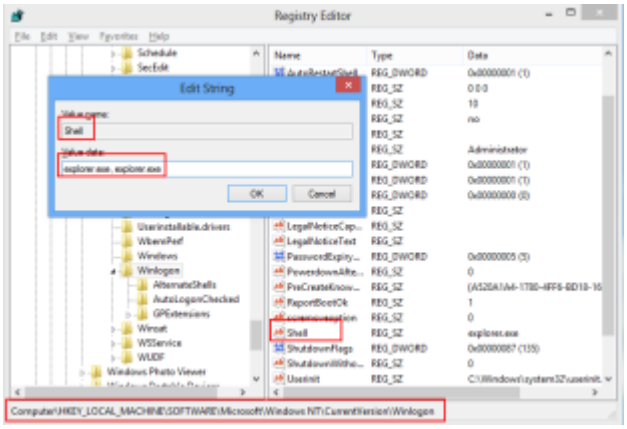
| Step | Details |
|---|---|
| **Step 12:** In the **Select I/O Controller Types** , leave the default selection. |  |
| **Step 13:** In the **Select a Disk Type** page, select **IDE** and click **Next**.<br>SCSI disks are not compatible with McAfee Advanced Threat Defense. |  |

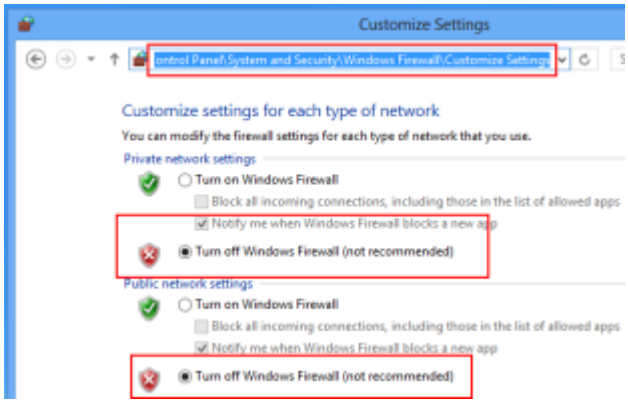
| Step | Details |
|---|---|
| **Step 14:** In the **Select a Disk** window, select **Create a new virtual disk** and click **Next**. |  |
| **Step 15:** Specify the details in the **Specify Disk Capacity** window and then click **Next**. | • **Maximum disk size (GB)** — For Windows 8 64-bit and 32-bit, the disk size can be 30 GB, however you must enter 24 GB for optimal performance.<br>• Select **Allocate all disk space now.**<br>• Select **Store virtual disk as a single file.**<br>  |

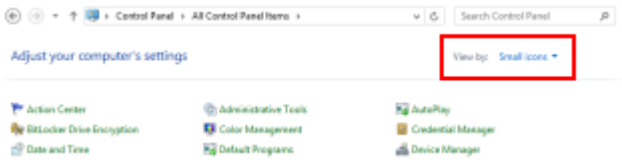
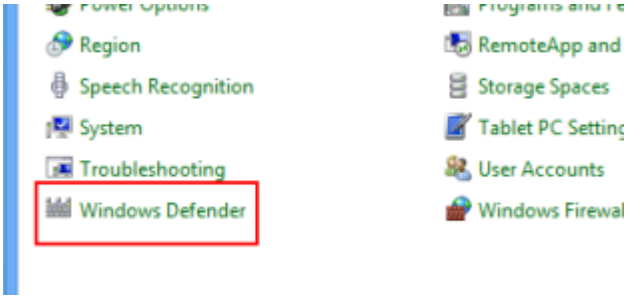
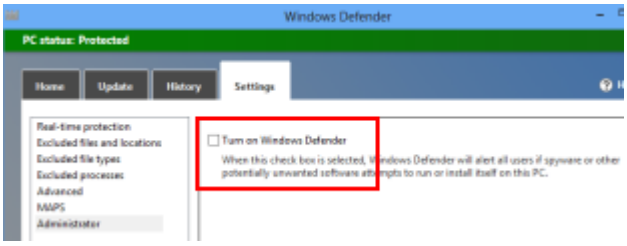
| Step | Details |
|---|---|
| **Step 16:** In the **Specify Disk file** window, make sure virtualMachineImage.vmdk is displayed by default and click **Next**.<br>If you specified a different name for **Virtual Machine name**, that name is displayed here. |  |

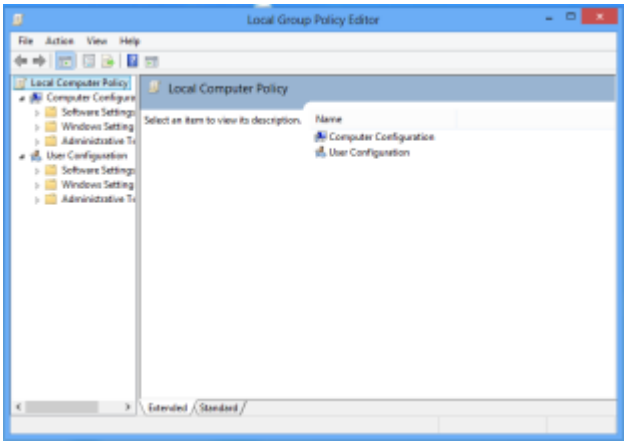
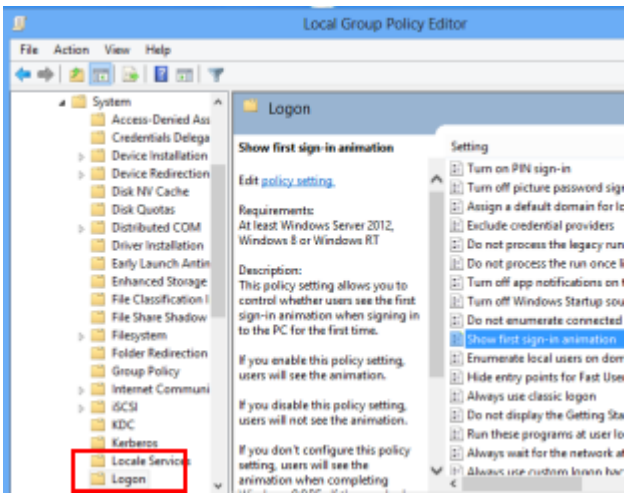
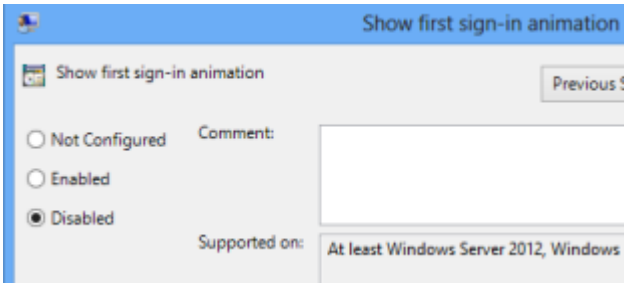
| Step | Details |
|---|---|
| **Step 17:** Complete the following in the **Ready to Create Virtual Machine** window. | • **Power on this virtual machine after creation** — Select this option.<br>• Click **Finish.**<br>This step might take around 30 minutes to complete.<br>  <br><br>  <br> |

| Step | Details |
|---|---|
| **Step 18:** If the **Removable Devices** pop-up window is displayed, select **Do not show this hint again** and click **OK**. | Windows begins to install, which might take around 15 minutes.<br>  |
| **Step 19**: Log on to virtualMachineImage using the following credentials:<br>• Administrator<br>• cr@cker42 |  |
| **Step 20:** The VM by default displays in the Metro UI mode. Click the Desktop tile to switch to Desktop mode. | |

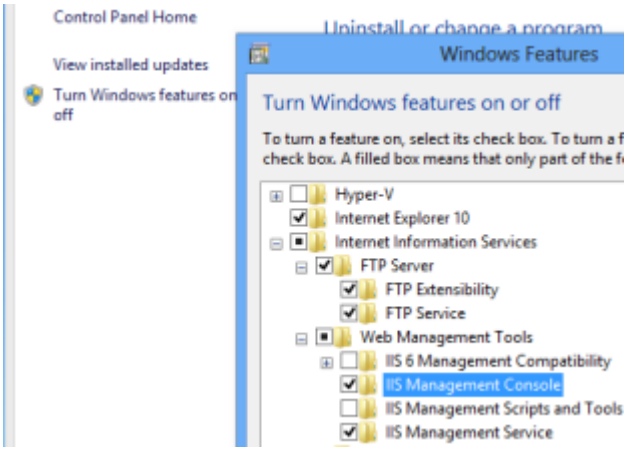
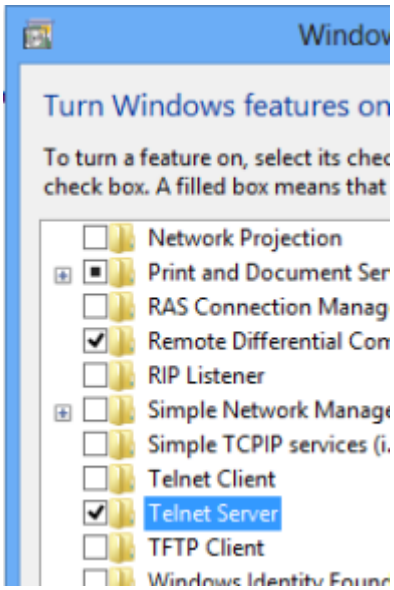
| Step | Details |
|---|---|
| **Step 21:** Set up Windows 8 to display in the Desktop mode instead of the default Metro UI mode when it starts. | 1 Press the Windows key and R simultaneously, which is the shortcut to open the **Run** dialog box.<br>2 In the **Run** dialog box, enter `regedit` and press Enter.<br>  <br>The **Registry Editor** opens.<br>3 Select **HKEY_LOCAL_MACHINE** \| **SOFTWARE** \| **Microsoft** \| **Windows NT** \| **CurrentVersion** \| **Winlogon** and then double-click on **Shell**.<br>4 Change **Value data** to `explorer.exe, explorer.exe` instead of the default value of `explorer.exe` and click **OK**.<br>  |

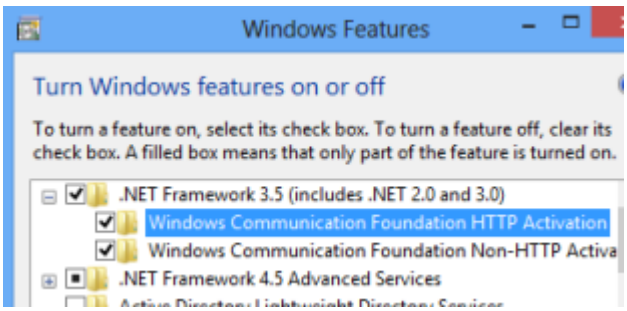
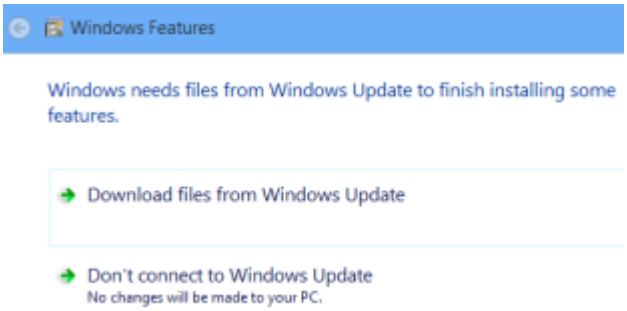
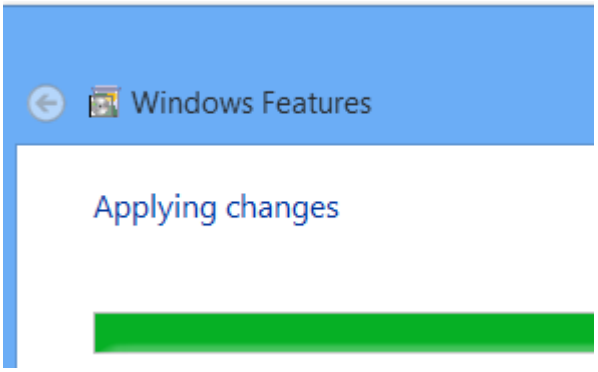
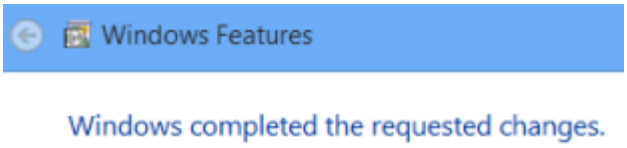
| Step | Details |
|---|---|
| **Step 22:** In the VM, turn off the Windows Firewall. | 1 Press the Windows key and X simultaneously and then select **Control Panel** \| **System and Security** \| **Windows Firewall** \| **Turn on Windows Firewall On or Off**.<br>2 Select **Turn off Windows Firewall (not recommended)** for both **Home or work(private) network location settings** and **Public network location settings** and then click **OK**.<br>  |

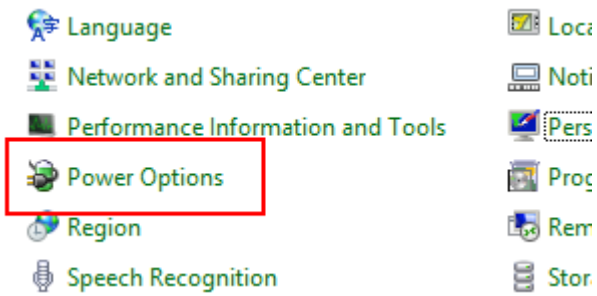
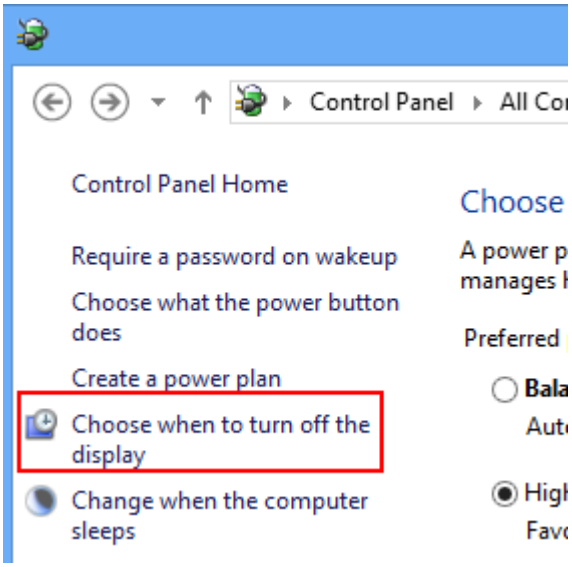
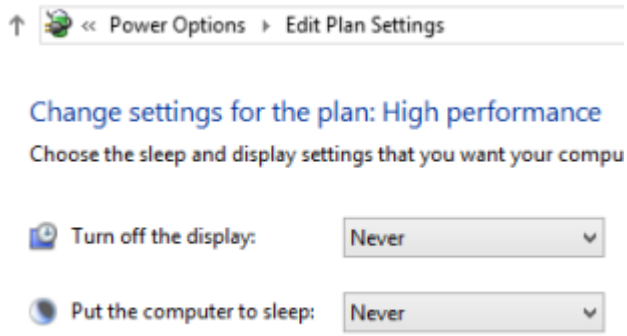
| Step | Details |
|---|---|
| **Step 23:** Disable Windows Defender. | 1 Open the Control Panel and from the **View by** drop-down select **Small Icons.**<br>  <br>2 Click **Windows Defender.**<br>  <br>3 In **Windows Defender**, select **Settings** \| **Administrators** and deselect **Turn on Windows Defender.** Then click **Save changes.**<br>  <br>4 Close the Windows Defender message box.<br> |

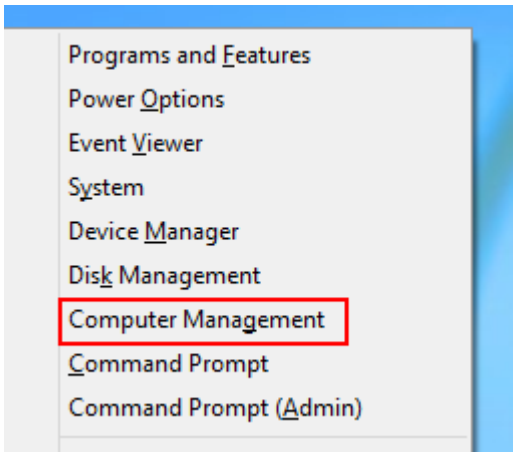
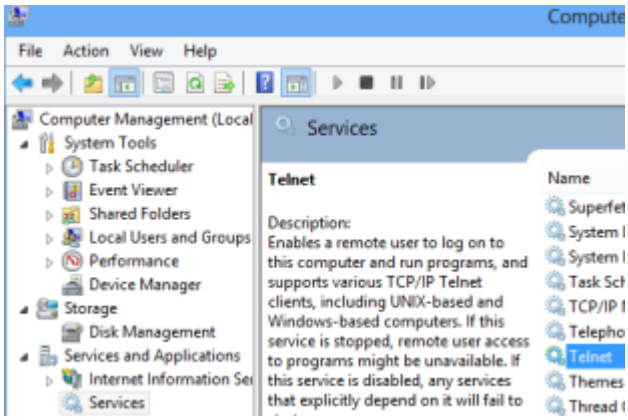
| Step | Details |
|---|---|
| **Step 24:** Disable first sign-in animation. | 1 Press the Windows key and R simultaneously, which is the shortcut to open the **Run** dialog box.<br>2 In the **Run** dialog box, enter `gpedit.msc` and press Enter. The **Local Group Policy Editor** opens.<br>  <br>3 Select **Computer Configuration** \| **Administrative Templates** \| **System** \| **Logon** and then open **Show first sign-in animation**.<br>  <br>4 Select **Disabled** and then click **OK**.<br>  |

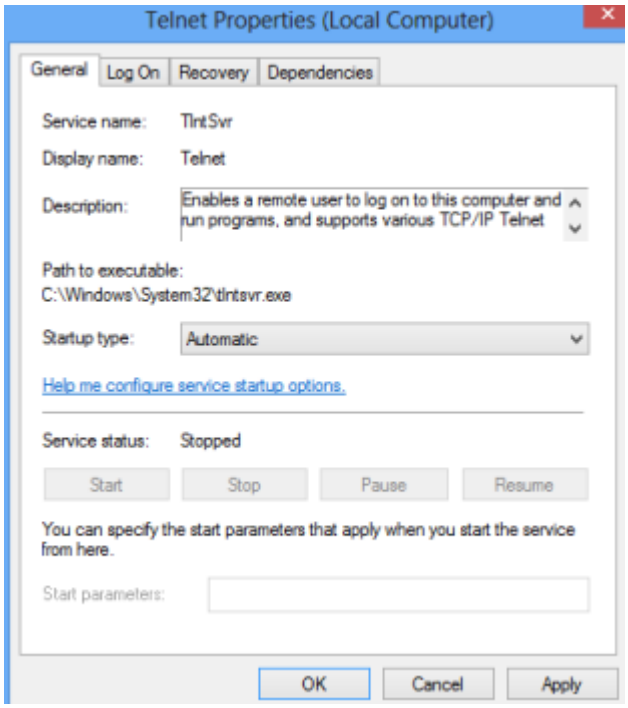
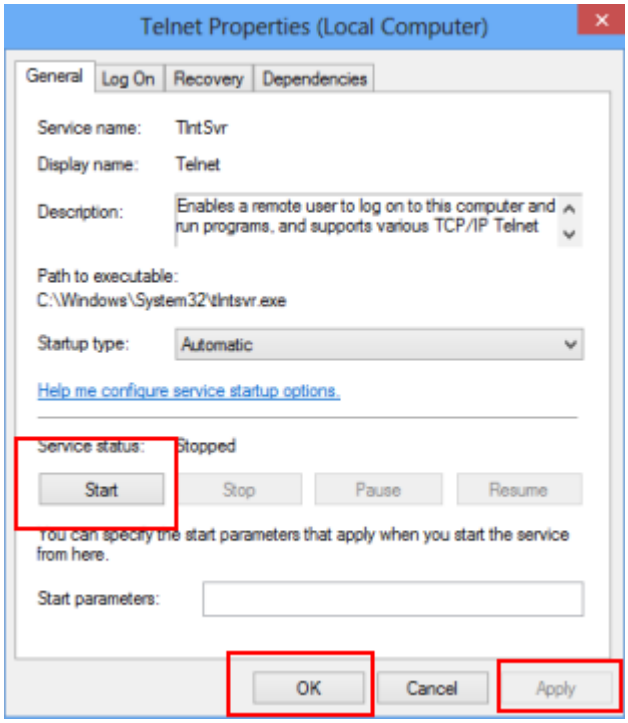
| Step | Details |
| --- | --- |
| | |

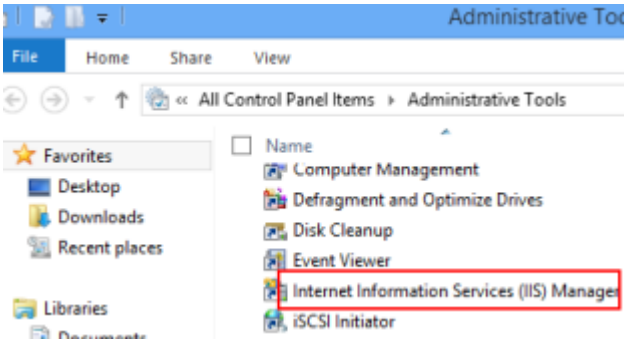
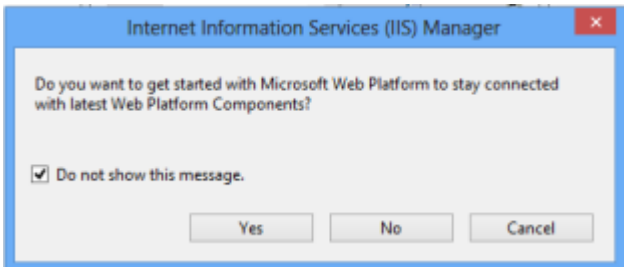
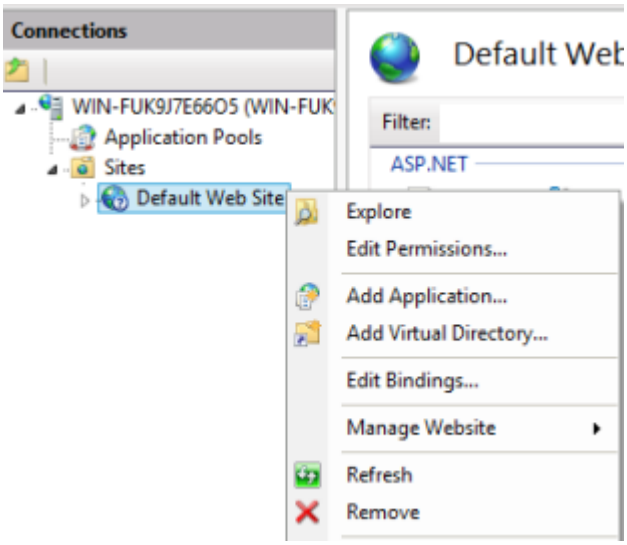
| Step | Details |
|---|---|
| **Step 25:** Press the Windows key and X simultaneously and then select **Control Panel** \| **Programs** \| **Programs and Features** \| **Turn Windows feature on or off** and complete the following. | 1 Select **Internet Information Services** \| **FTP server** and select **FTP Extensibility**.<br>2 Select **Internet Information Services** \| **Web Management Tools** and select **IIS Management Console** and **IIS Management Service**.<br>  <br>3 Select **Telnet Server.**<br>  <br>4 Select **.NET Framework 3.5(includes .NET 2.0 and3.0)** and then select **Windows Communication Foundation HTTP Activation** and **Windows Communication Foundation Non-HTP Activation** options. |

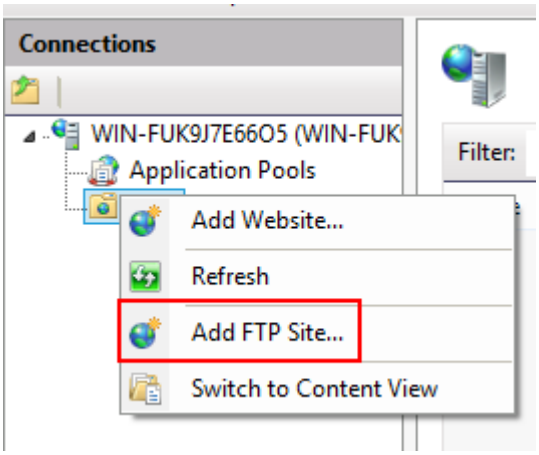
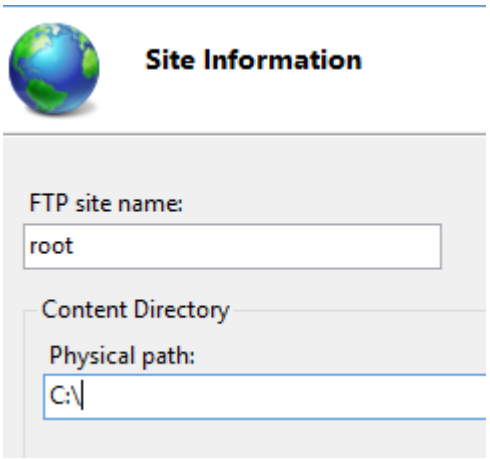
| Step | Details |
|---|---|
| |  <br>5 Press **OK**.<br>6 If the following message is displayed, select **Download files from Windows Update.**<br>  <br>This operation might take around 5 minutes to complete.<br>  <br>A confirmation message is displayed when the operation completes.<br>  |

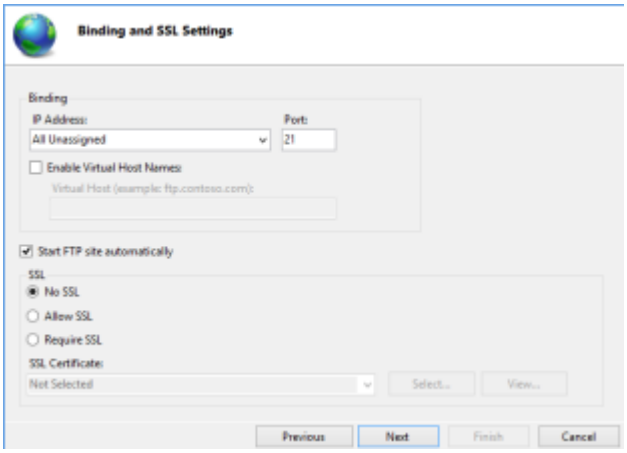
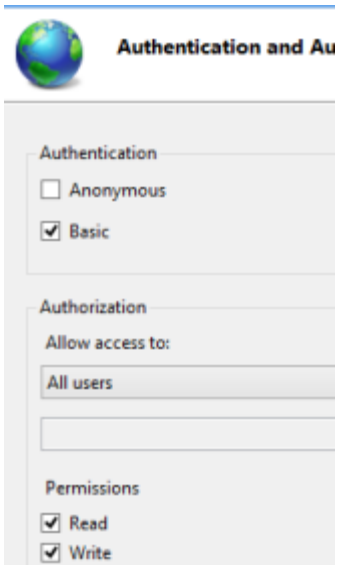
| Step | Details |
|---|---|
| **Step 26:** Edit the power options. | 1 Open the Control Panel and from the **View by** drop-down select **Small Icons.**<br>2 Click **Power Options.**<br>  <br>3 Click **Choose when to turn off the display.**<br>  <br>4 Select **Never** for **Turn off the display** and **Put the computer to sleep** and then click **Save changes.**<br>  |

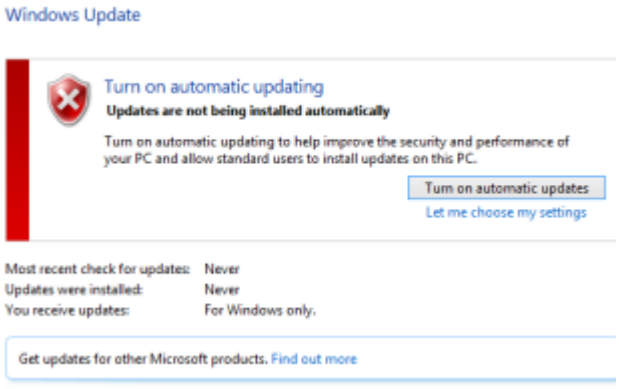
| Step | Details |
|---|---|
| | |
| **Step 27:** Press the Windows key and X simultaneously and then select **Computer Management** \| **Services and Applications** \| **Services.** Then double-click on **Telnet.** |  <br>  |

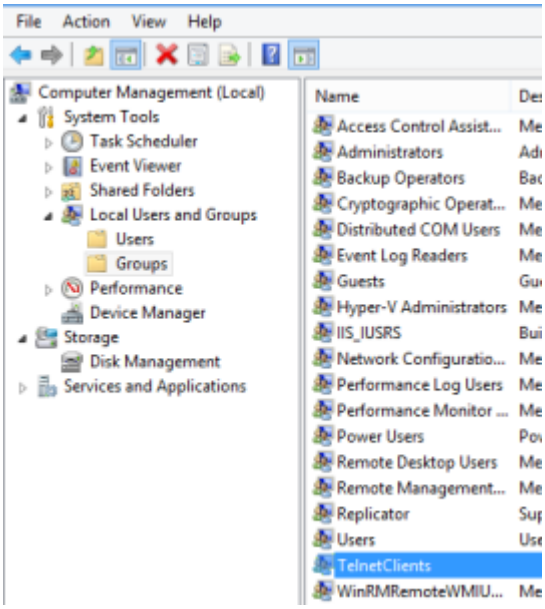
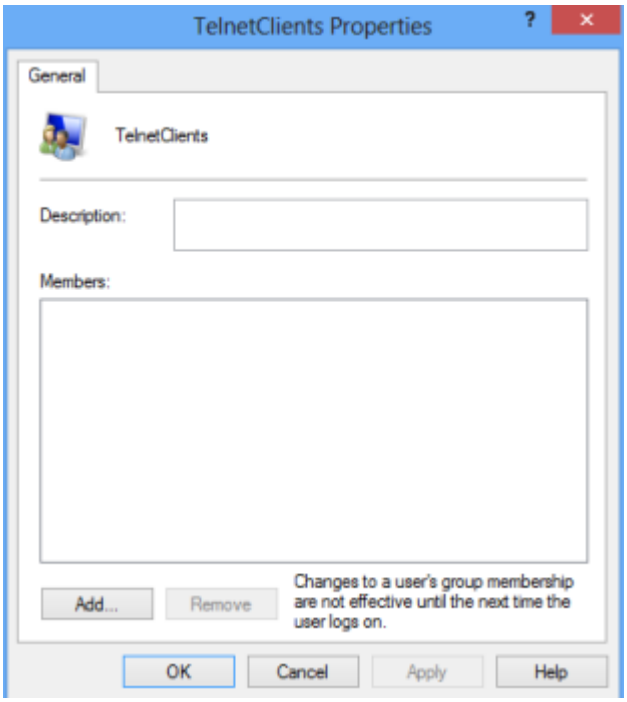
| Step | Details |
|---|---|
| **Step 28:** In the Telnet Properties (Local Computer) dialog, select **Automatic** from the **Startup type** list. Then select **Apply** \| **Start** \| **OK**. |  <br>  |

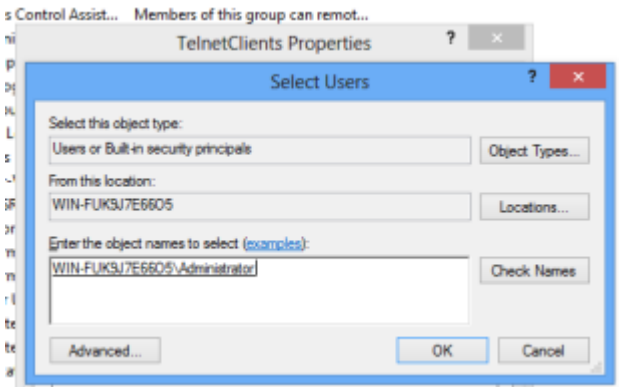
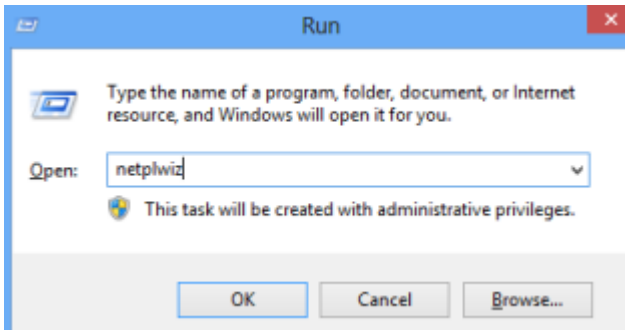
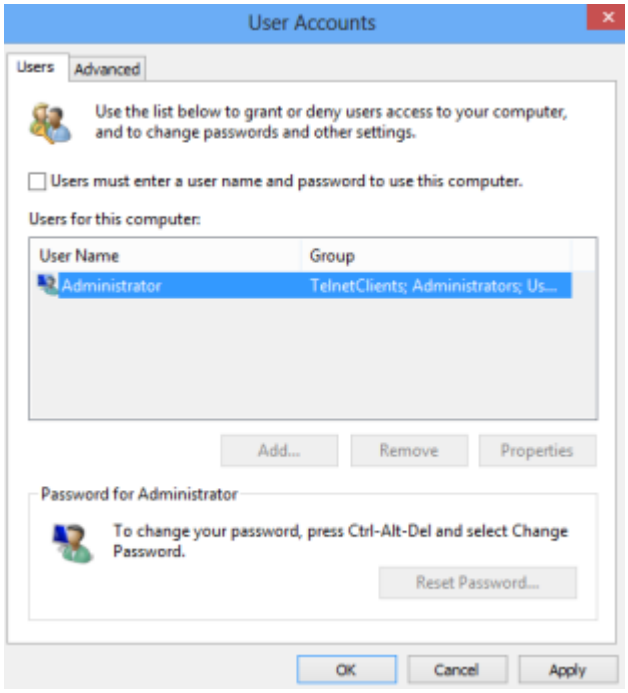
| Step | Details |
|---|---|
| **Step 29:** Enable FTP on Windows 8. | 1 Press the Windows key and X simultaneously and then select **Control Panel** \| **System and Security** \| **Administrative Tools**.<br>  <br>2 Double-click **Internet Information Services(IIS) Manager**, expand the tree under **Hostname**.<br>3 If you see the following message box, select **Do not show this message** and click **Cancel**.<br>  <br>4 Select **Sites** and right-click **Default Web Site** and then select **Remove**. Confirm by clicking **Yes**.<br>  |

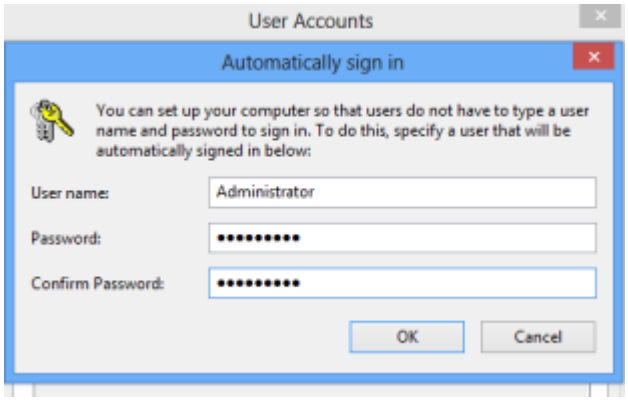
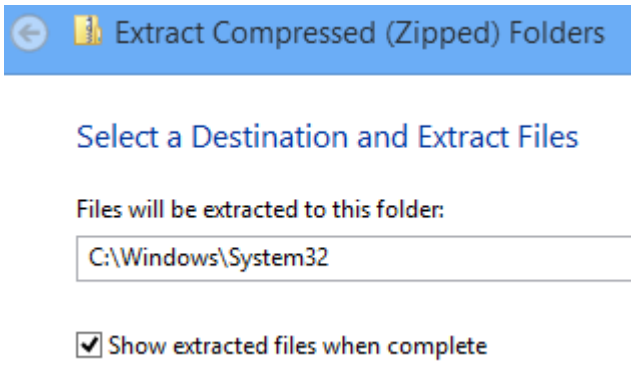
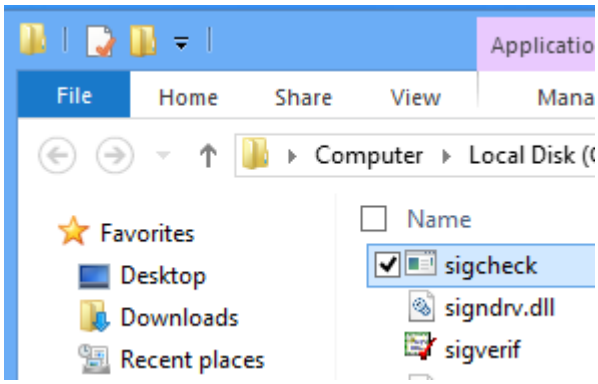
| Step | Details |
|---|---|
| | 5 Right-click **Sites** and select **Add FTP Site.** Then complete the following.<br>  <br>a For **FTP site name**, enter `root`.<br>b **Physical Path: C:\.**<br>c Click **Next.**<br>  <br>6 For **Bindings and SSL Settings**, select **No SSL**. For all other fields, leave the default values and click **Next.** |

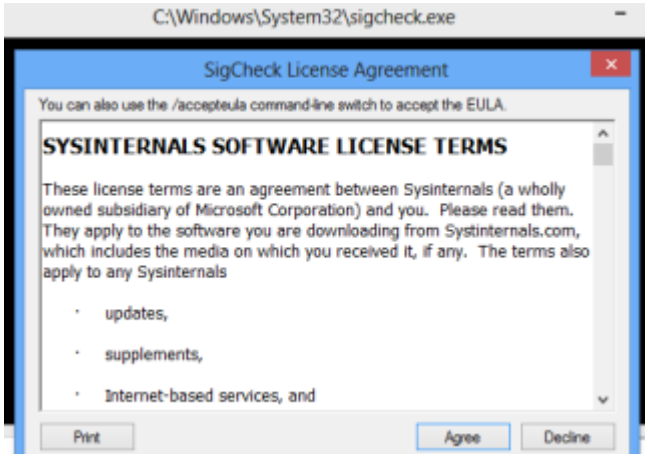
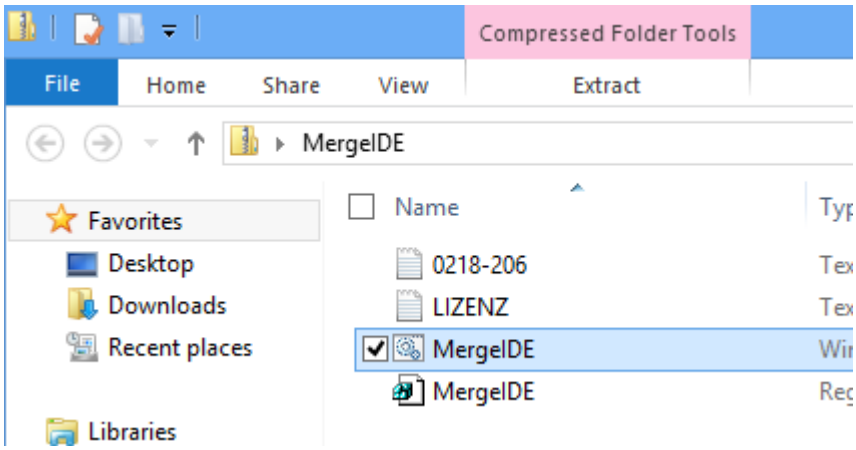
| Step | Details |
|---|---|
| |  <br>7 For **Authentication and Authorization Information** complete the following.<br>**a** Select **Basic**.<br>**b** For **Allow access to**, select **All Users**.<br>**c** For **Permissions**, select both **Read** and **Write**, and then click **Finish**.<br>**d** Close the **Internet Information Services (IIS) Manager**.<br>  |

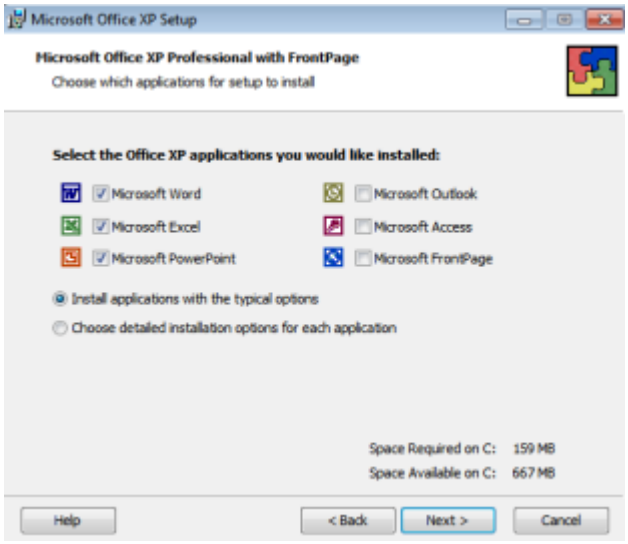
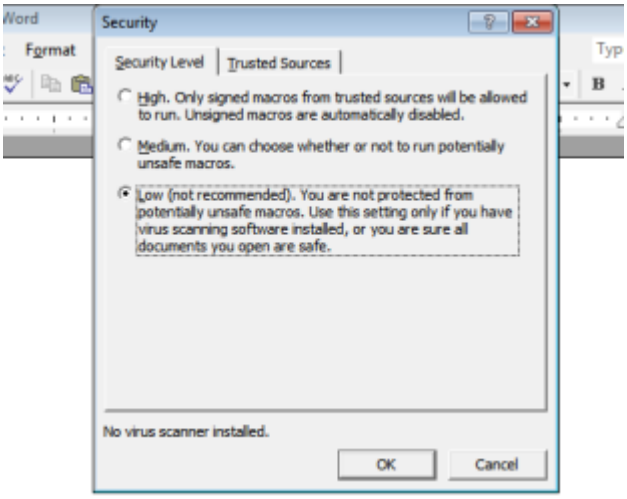
| Step | Details |
|---|---|
| **Step 30:** Turn off automatic updating for Windows. | 1 Press the Windows key and X simultaneously and then select **Control Panel** \| **Windows Update** \| **Change**.<br>2 Select **Never check for updates (not recommended)** and click **OK**.<br>  |

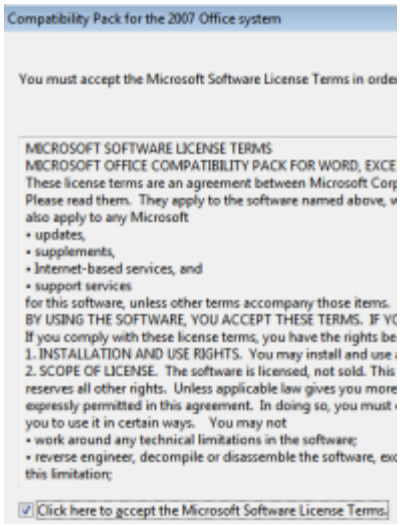
| Step | Details |
|---|---|
| **Step 31:** Complete the following:<br>1 Open the Control Panel and from the **View by** drop-down select **Small Icons**.<br>2 Select **Administrator Tools** \| **Computer Management** and complete the steps in the next column. | 1 Select **Computer Management (Local)** \| **System Tools** \| **Local Users and Groups** \| **Groups**<br>  <br>2 Double-click **TelnetClients**.<br>  <br>3 Click **Add** and enter `Administrator`.<br>4 Click **Check Names** and then **OK**. |

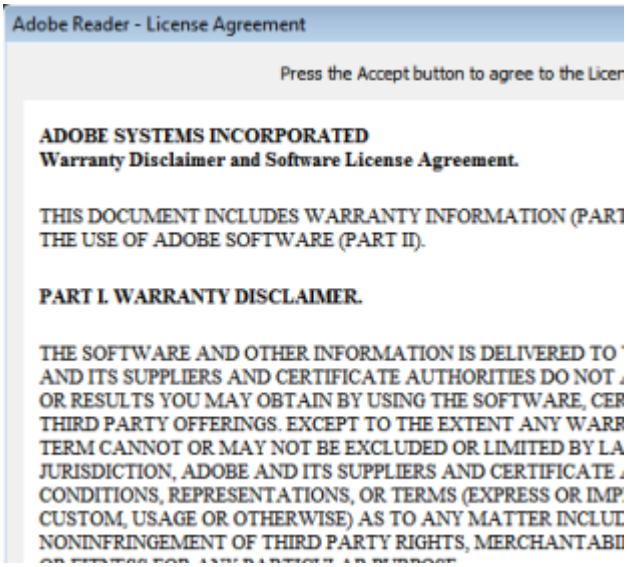
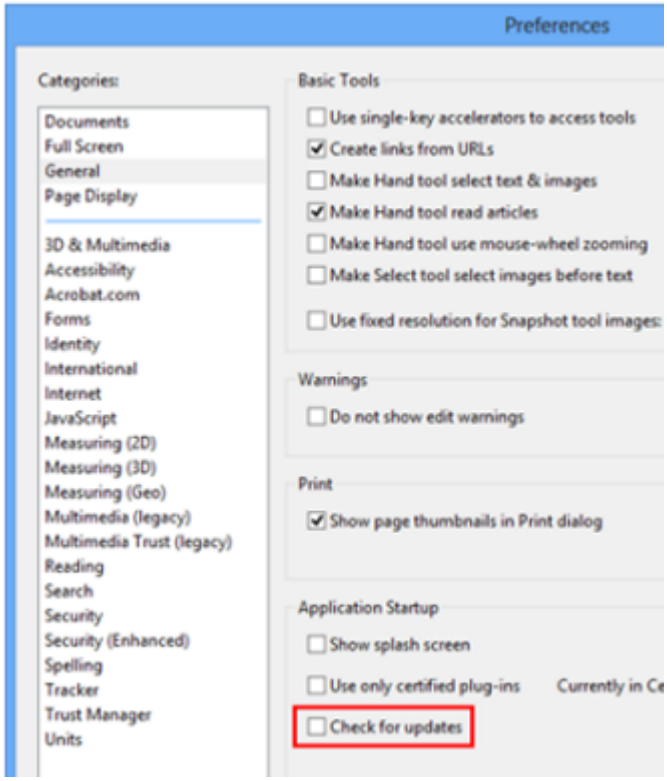
| Step | Details |
|---|---|
| |  |
| **Step 32:** Press the Windows key and R simultaneously, which is the shortcut to open the **Run** dialog box. Then enter `netplwiz` and click **OK**. |  |
| **Step 33:** In the **User Accounts** window, deselect **Users must enter a user name and password to use this computer** and click **Apply**. |  |

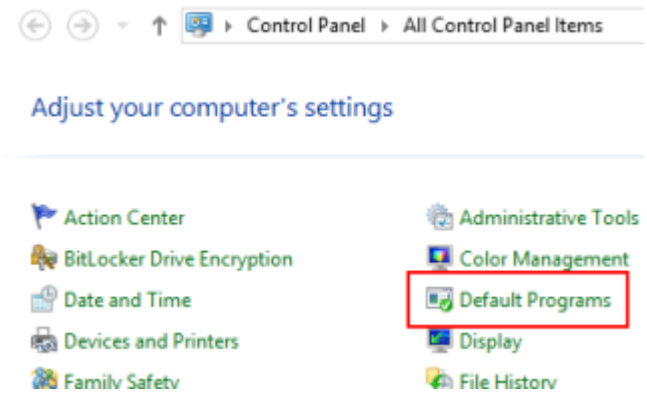
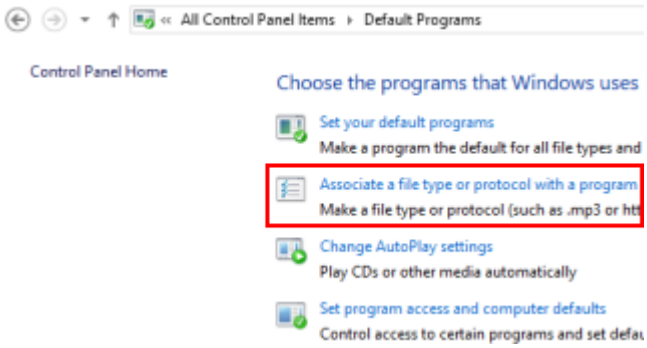
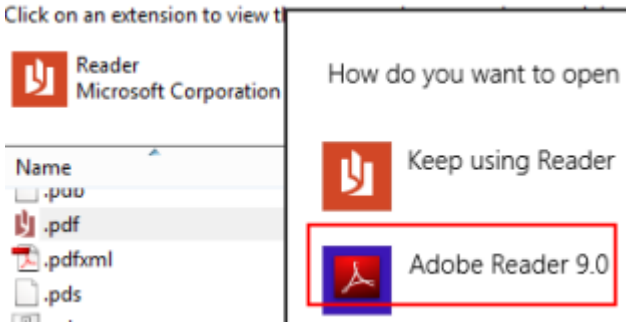
| Step | Details |
|---|---|
| **Step 34:** In the **Automatically sign in** pop-up window, complete the following and then press **OK** in the message boxes. | • **User name** — Enter `Administrator`<br>• **Password** — Enter `cr@cker42`<br>• **Confirm Password** — Enter `cr@cker42`<br>  |
| **Step 35:** Download Sigcheck on to your computer (the native host) from http://technet.microsoft.com/en-us/sysinternals/bb897441.aspx. | The VM that you created has the Windows Firewall switch off as well as there is no anti-virus installed on it. Therefore, it is recommended that you download the programs and components on to the native host first and then copy them to the VM in VMware Workstation. |
| **Step 36:** Extract sigcheck.zip to `C:\WINDOWS\system32` location. |  |
| **Step 37:** In Windows Explorer, go to C:\WINDOWS\system32 and double-click **sigcheck.exe**. |  |

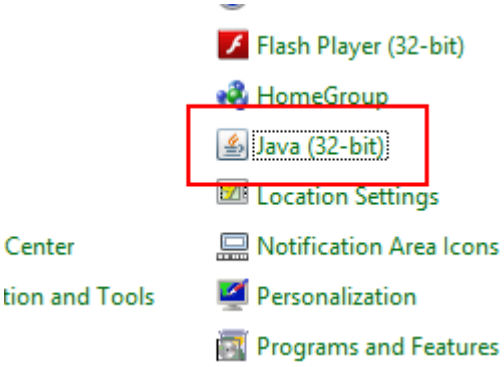
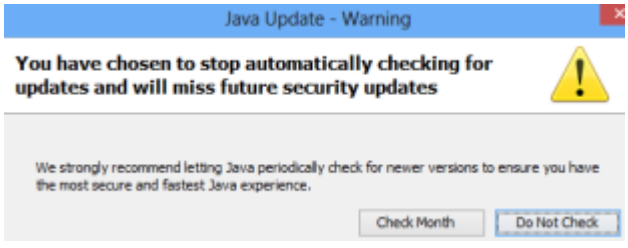
| Step | Details |
|---|---|
| **Step 38:** Click **Agree** for **Sigcheck License Agreement.**<br><br>After you click on **Agree**, no confirmation message is displayed. |  |
| **Step 39:** Download MergeIDE.zip from https://www.virtualbox.org/attachment/wiki/Migrate_Windows/MergeIDE.zip on to the native computer and then copy it to the VM. | |
| **Step 40:** Extract MergeIDE.zip and run the MergeIDE batch file in the VM. |  <br>• If prompted, select **Run** in the warning message.<br>• Close Windows Explorer. |

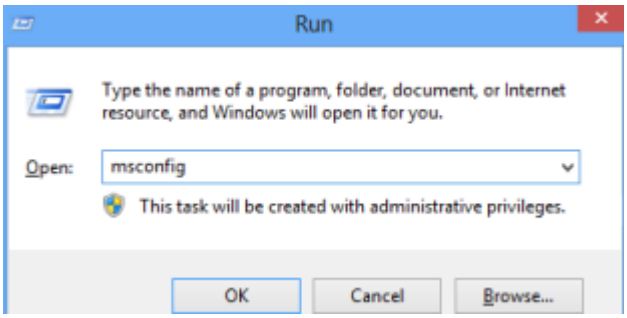
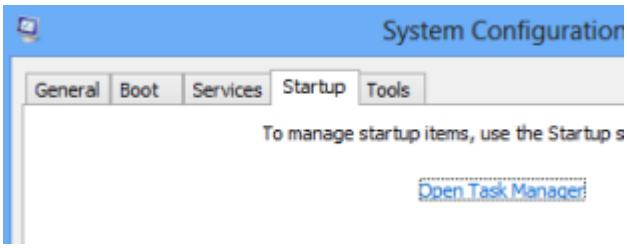
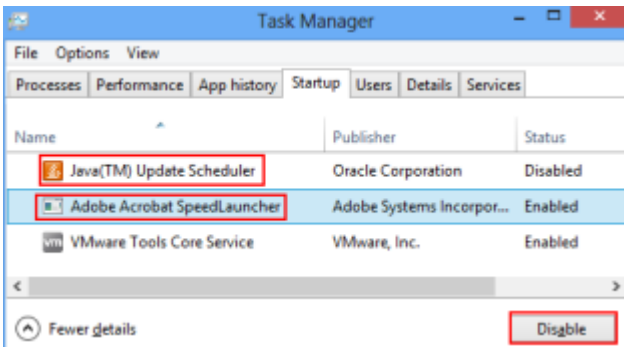
| Step | Details |
|---|---|
| **Step 41:** To analyze Microsoft Word, Excel, and Powerpoint files, install Microsoft Office 2003 on the virtual machine. |  |
| **Step 42:** Lower the security to run macros for the Office applications. | • Open Microsoft Word 2003 and select **Tools** \| **Macro** \| **Security** and then select **Low** and click **OK**.<br>  <br>• Similarly lower the macro security for Microsoft Excel and PowerPoint. |

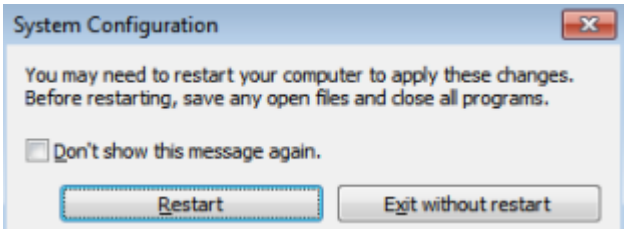
| Step | Details |
|---|---|
| **Step 43:** You need the compatibility pack to open Microsoft Office files that were created in a newer version of Microsoft Office. For example, to open a .docx file using Office 2003, you need the corresponding compatibility pack installed.<br>Go to http://www.microsoft.com/en-us/download/details.aspx?id=3 and download the required Microsoft Office compatibility pack for Word, Excel, and PowerPoint File Formats. Then install them on the virtual machine. | In the **Compatibility Pack for the 2007 Office system** dialog, select **Click here to accept the Microsoft Software License Terms** and click **Continue.**<br>  |

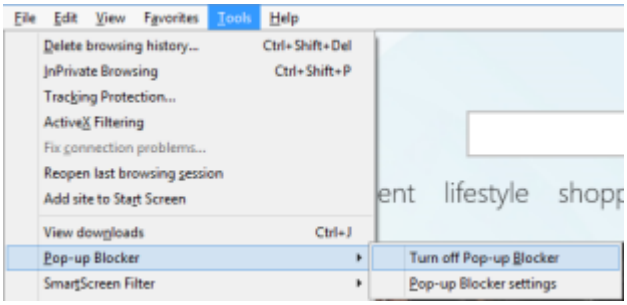
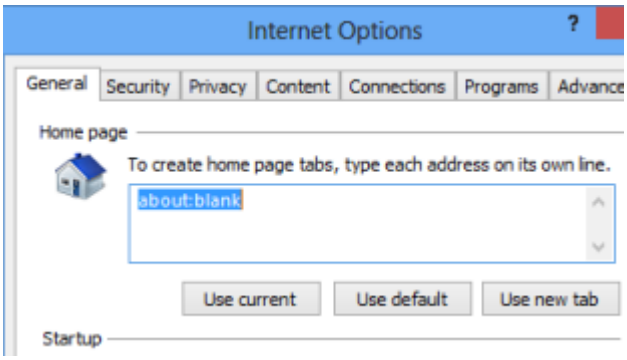
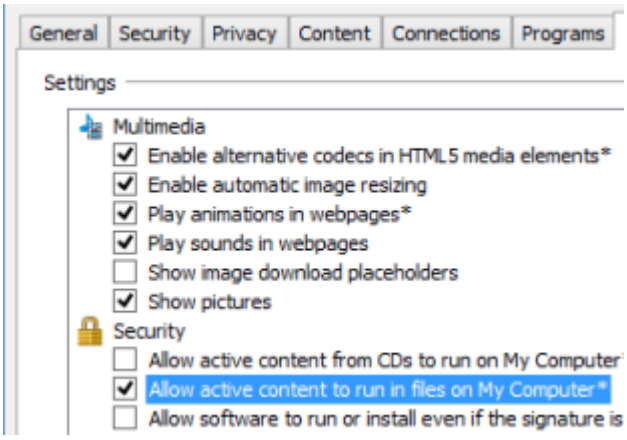
| Step | Details |
|---|---|
| **Step 44:** To analyze PDF files, download Adobe Reader to the native host and copy it to the VM.<br><br>This procedure uses Adobe Reader 9.0 as an example. | 1 Install Adobe Reader 9.0 in the VM.<br><br>2 Open Adobe Reader and click **Accept**.<br><br>  <br><br><br>3 In Adobe Reader, select **Edit** \| **Preferences** \| **General** and deselect **Check for updates**.<br><br>  <br> |

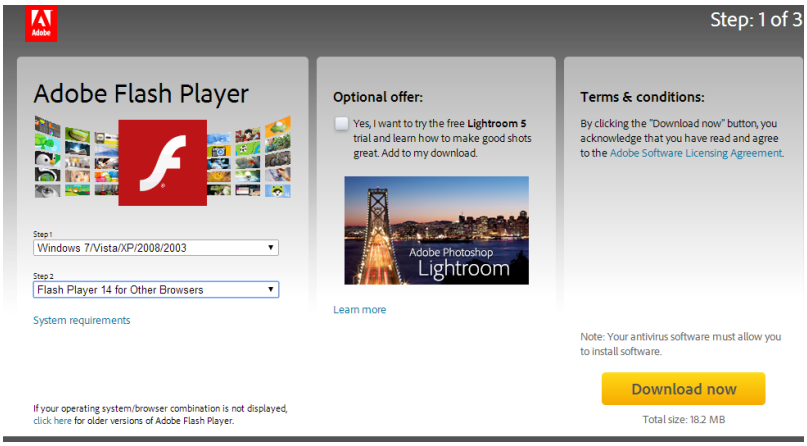
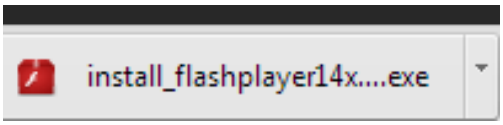
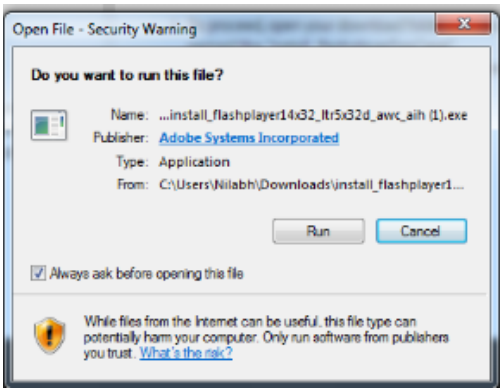
| Step | Details |
|---|---|
| **Step 45:** Set Adobe Reader 9 as the default application to open PDF files. | 1 In the **Control Panel** (icons view), select **Default Programs.**<br>  <br>2 Select **Associate a file type or protocol with a program**<br>  <br>3 Locate **.pdf** and double click on it. Chose Adobe Reader 9.0 as the default PDF reader.<br>  |

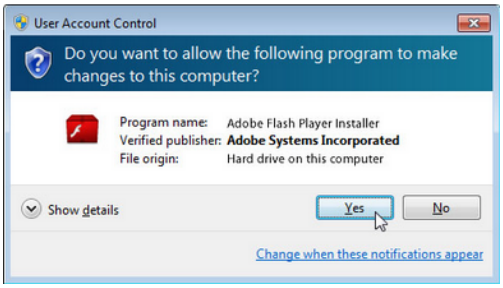
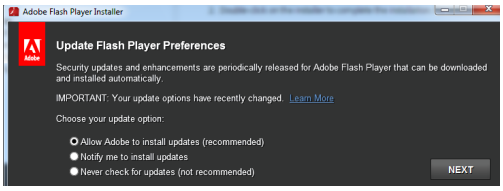
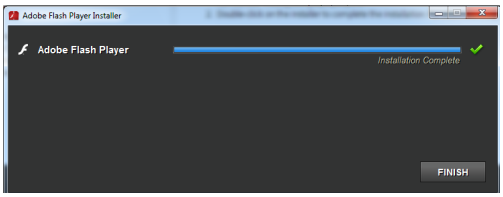
| Step | Details |
|---|---|
| **Step 46:** To analyze JAR files, download and install Java Runtime Environment.<br><br>This procedure uses Java 7 Update 25 as an example. | |
| **Step 47:** Open Java in Control Panel. |  |
| **Step 48:**In the **Update** tab, deselect **Check for Updates Automatically.** | |
| **Step 49:** In the Java Update Warning dialog, select **Do Not Check** and then click **OK** in the Java Control Panel. |  |

| Step | Details |
|---|---|
| **Step 50:** Disable *jusched* and *reader_sl*. | 1 Press the Windows key and R simultaneously, which is the shortcut to open the **Run** dialog box. In the Windows Run dialog, enter `msconfig` and click **OK**.<br>  <br><br>2 In the **System Configuration** utility, go to the **Startup** tab.<br>  <br><br>3 Click **Open Task Manager.**<br>4 If *Java(TM) Update Scheduler* (jusched) is listed, select it and click **Disable.**<br>5 If *Adobe Acrobat SpeedLauncher* (reader_sl) is listed, select it and click **Disable.**<br>  <br><br>6 In the **System Configuration** dialog, select **Don't show this message again** and click **Restart.** |

| Step | Details |
| --- | --- |
| |  |

| Step | Details |
|---|---|
| **Step 51:** Open the default browser and set it up for malware analysis.<br><br>This procedure uses Internet Explorer as an example. | 1 Make sure the pop-up blocker is turned off. In Internet Explorer, select **Tools** \| **Pop-up Blocker** \| **Turn off Pop-up Blocker.**<br><br>  <br><br>2 Select **Tools** \| **Internet Options** and for **Home page** enter `about:blank`.<br><br>  <br><br>3 Go to the **Advanced** tab of the Internet Options and locate **Security.**<br><br>4 Select **Allow active content to run in files on My Computer.**<br><br>  <br><br>5 Click **OK.** |

| Step | Details |
|---|---|
| **Step 52:** To dynamically analyze Flash files (SWF), install the required version of Adobe Flash.<br><br>This procedure uses Flash Player 14 as an example. | 1 Goto http://get.adobe.com/flashplayer/otherversions/.<br><br>2 Select Operating System and Flash Player version respectively as per your requirement in **Step 1** and **Step 2** drop-down as shown below.<br><br>3 Click on **Download now** tab.<br><br>  <br><br>4 Double-click the Adobe Flash Player Installer file **(install_flashplayer xxx.exe)**, present at the bottom corner of your screen.<br><br>  <br><br>5 In the**Security Warning dialogue box**, Click **Run**.<br><br>  <br><br>6 In the **User Account Control** dialogue box, Click **Yes**. |

| Step | Details |
|---|---|
| |  <br>7 Choose your update option and Click **NEXT**.<br>  <br>8 Click **FINISH** to complete Adobe Flash Player installation.<br>  |
| **Step 53:** Shut down the VM. | |
| **Step 54:** Go to the location that you provided in step 8 to find the VMDK file named as `virtualMachineImage-flat.vmdk` | If you require, you can rename this VMDK file as Windows 8 x64-flat.vmdk or Windows 8 x32-flat.vmdk. |

# Import a VMDK file into McAfee Advanced Threat Defense

**Before you begin**

- You have the VMDK file at hand.
- The operating system of the VM is activated and it has all the applications that you require, such as Microsoft Office applications, Adobe PDF Reader, and so on.
- The VMDK file does not contain any spaces in its file name. If it contains any spaces, the VMDK to image file conversion will fail subsequently.

To create an analyzer VM, you must first import the corresponding VMDK file into McAfee Advanced Threat Defense. By default, you can use only SFTP to import the VMDK file. To use FTP, you must enable it using the `set ftp` CLI command. See set ftp on page 314.

Generally, FTP transfer is faster than SFTP but less secure than SFTP. If your Advanced Threat Defense Appliance is placed in an unsecured network, such as an external network, McAfee recommends you to use SFTP.

### Task

1 Open an FTP client.

For example, you can use WinSCP or FileZilla.

2 Connect to the FTP server on McAfee Advanced Threat Defense using the following credentials.

- Host: IP address of McAfee Advanced Threat Defense.
- Username: atdadmin
- Password: atdadmin
- Port: The corresponding port number based on the protocol you want to use.

3 Upload the VMDK file from the local machine to McAfee Advanced Threat Defense.

# Convert the VMDK file to an image file

**Before you begin**

- You have uploaded the VMDK file to McAfee Advanced Threat Defense.
- You have admin-user permissions in McAfee Advanced Threat Defense.

### Task

1 In the McAfee Advanced Threat Defense web application, select **Manage** | **Image Management**.

2 In the **Image Management** page, select the VMDK file that you imported from the **VMDK Image** drop-down.

3 Provide a name to the image file.

The name that you provide must be between 1 and 20 characters in length and must not contain any spaces. If the image name contains a space, then the conversion to image file fails.

For malware analysis, you might require multiple analyzer VMs that run on the same operating system but with different applications. For example, you might require a Windows 7 SP1 analyzer VM with Internet Explorer 10 and another Windows 7 SP1 analyzer VM with Internet Explorer 11. If you plan to create multiple analyzer VMs of the same operating system, it is mandatory that you provide an **Image Name**. If you plan to create only one analyzer VM for a specific operating system, then providing the **Image Name** is optional. If you do not provide a name, a default name is assigned to the image file, which you use to view the logs, create VM profile, and so on.

The default names for the image files are as follows:

- **winXPsp2**: corresponds to Microsoft Windows XP 32-bit Service Pack 2
- **winXPsp3**: corresponds to Microsoft Windows XP 32-bit Service Pack 3
- **win7sp1**: corresponds to Microsoft Windows 7 32-bit Service Pack 1

- **win7x64sp1**: corresponds to Microsoft Windows 7 64-bit Service Pack 1
- **win2k3sp1**: corresponds to Microsoft Windows Server 2003 32-bit Service Pack 1
- **win2k3sp2**: corresponds to Microsoft Windows Server 2003 32-bit Service Pack 2
- **win2k8sp1**: corresponds to Microsoft Windows Server 2008 R2 Service Pack 1
- **win8p0x32**: corresponds to Microsoft Windows 8 32-bit
- **win8p0x64**: corresponds to Microsoft Windows 8 64-bit

The name that you provide is appended to the default name. Suppose you provide *with_PDF* as the **Image Name** and the operating system is Windows Server 2003 32-bit Service Pack 1. Then the image file is named as *win2k3sp1_with_PDF*.

If you attempt to create multiple analyzer VMs of the same operating system, then every time the image file is named using the default name for the operating system. Therefore, the same image file is overwritten every time instead of creating a new analyzer VM of the same operating system. This is why it is mandatory to provide **Image Name** when creating multiple analyzer VMs of the same operating system.

4 Select the corresponding operating system from the **Operating System** drop-down.

5 Click **Convert**.

The time taken for this conversion depends on the size of the VMDK file. For a 15 GB file, an ATD-3000 might take around five minutes.

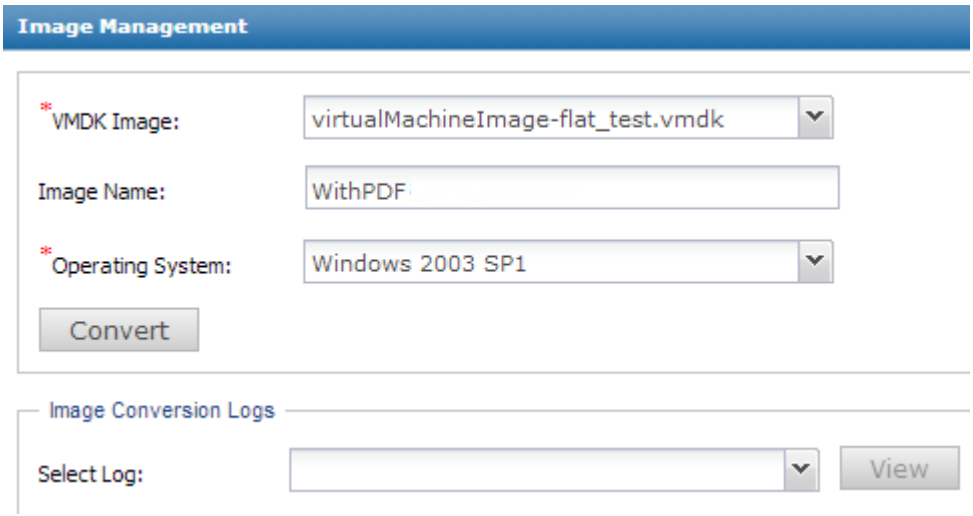



**Figure 5-2 VMDK to image file conversion**

After the conversion is complete, a message is displayed.

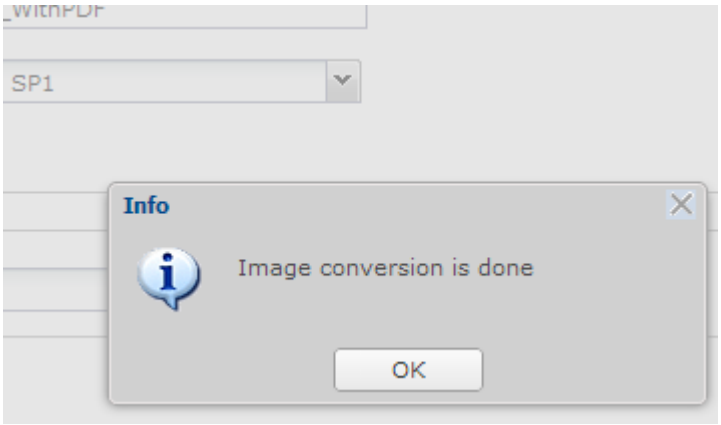



**Figure 5-3 Confirmation message**

6 To view the logs related to image conversion, select the image name from the **Select Log** list and click **View**.

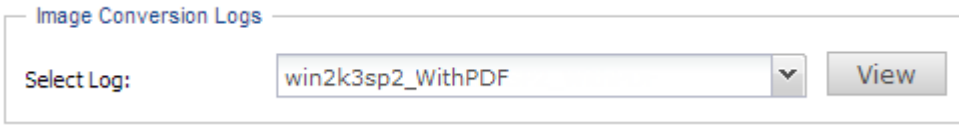



**Figure 5-4 Select the image file to view the logs**

If you had not provided the **Image Name**, then the image file is assigned the default name based on the operating system. If you had provided an **Image Name**, the name that you provided is appended to the default name.

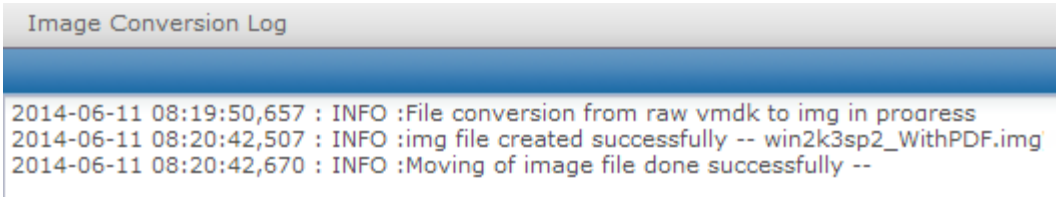


Image Conversion Log
2014-06-11 08:19:50,657 : INFO :File conversion from raw vmdk to img in progress
2014-06-11 08:20:42,507 : INFO :img file created successfully -- win2k3sp2_WithPDF.img
2014-06-11 08:20:42,670 : INFO :Moving of image file done successfully --

**Figure 5-5 Image conversion log entries**

# Managing VM profiles

After you convert the imported VMDK file to an image file, you create a VM profile for that image file.

You cannot associate this VM profile with any other image file. Similarly, once associated, you cannot change the VM profile for an image file.

VM profiles contain the operating system and applications in an image file. This enables you to identify the images that you uploaded to McAfee Advanced Threat Defense and then use the appropriate image for dynamically analyzing a file. You can also specify the number of licenses that you possess for the operating system and the applications. McAfee Advanced Threat Defense factors this in when creating concurrent analyzer VMs from the corresponding image file.

You use the McAfee Advanced Threat Defense web application to manage VM profiles.

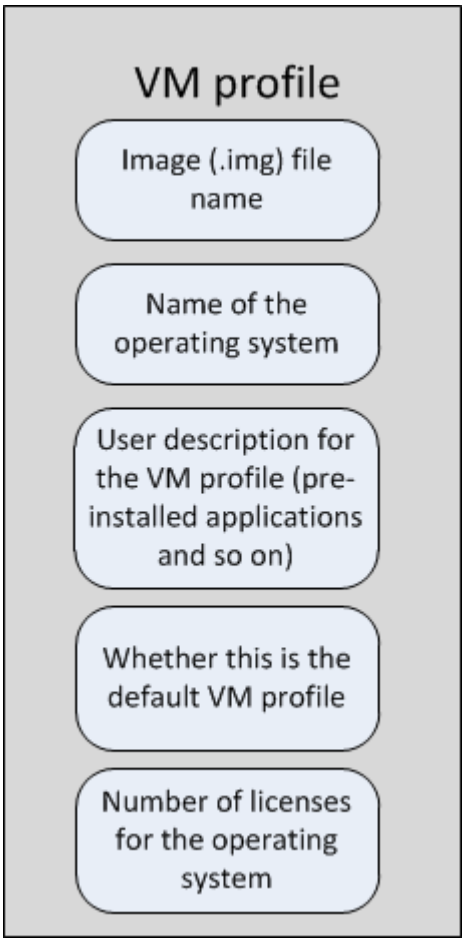

VM profile
Image (.img) file name
Name of the operating system
User description for the VM profile (pre-installed applications and so on)
Whether this is the default VM profile
Number of licenses for the operating system

**Figure 5-6 Configurations in a VM profile**

## View VM profiles

You can view the existing VM profiles in the McAfee Advanced Threat Defense web application.

### Task

1 Select **Policy | VM Profile.**

The currently available VM profiles are listed.

| Column name | Definition |
|---|---|
| **Select** | Select to edit or delete the corresponding VM profile. |
| **Name** | Name that you have assigned to the VM profile. |
| **Licenses** | The number of end-user licenses that you possess for the corresponding operating system and applications. This is one of the factors that determine the number of concurrent analyzer VMs on McAfee Advanced Threat Defense. |
| **Default** | Whether this is a default VM profile. |
| **Size** | The size of the image file in megabytes. |
| **Hash** | The MD5 hash value of the image file. |

2 Hide the unneeded columns.

a Move the mouse over the right corner of a column heading and click the drop-down arrow.

b Select **Columns**.

c Select only the required column names from the list.

You can click a column heading and drag it to the required position.

3 To sort the records based on a particular column name, click the column heading.

You can sort the records in the ascending or descending order. Alternatively, move the mouse over the right corner of a column heading and click the drop-down arrow. Then select **Sort Ascending** or **Sort Descending**.

4 To view the complete details of a specific VM Profile, select the record and click **View**.

## Create VM profiles

After you have converted the VMDK file to the image format, you can initiate the VM creation and also create the corresponding VM profile.

Each image file that you converted must be associated with only one VM profile. That is, you need one unused image file for each VM profile that you want to create. However, you can convert the same VMDK file image files multiple times. This enables you to create multiple image files from one VMDK file.

### Task

1 Select **Policy** | **VM Profile** | **New.**.

The **VM Profile** page is displayed.

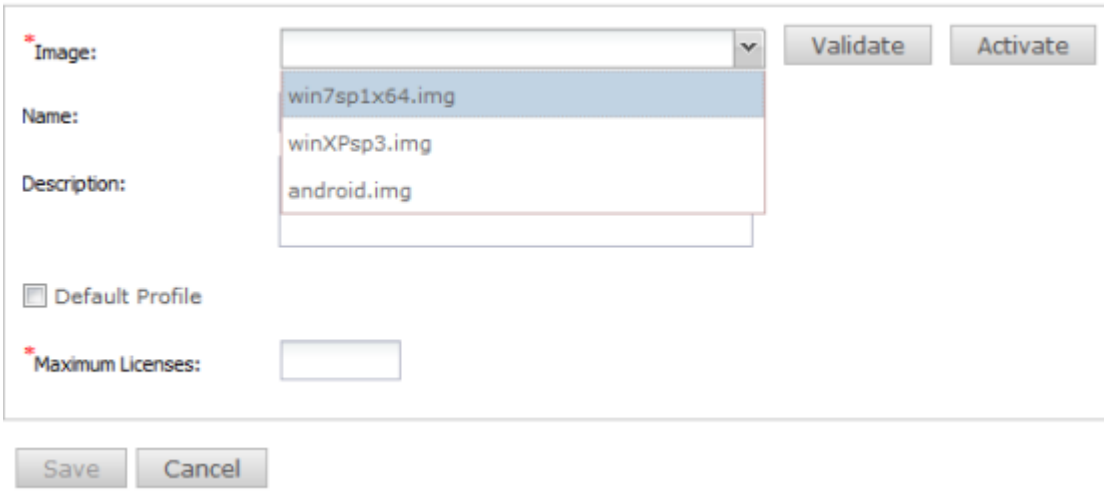



**Figure 5-7 Select the image file**

2 From the **Image** drop-down, select the one for which you want to create the VM profile.

3 Click **Activate** to create the VM from the selected image file.

- When you click **Activate**, the VM is opened in a pop-up window. So, make sure pop-up blocker is not enabled on your browser.
- This is not related to Windows activation with Microsoft. You must complete Windows activation before you import the VMDK file into McAfee Advanced Threat Defense using FTP or SFTP.

A progress bar indicating the VM creation is displayed.

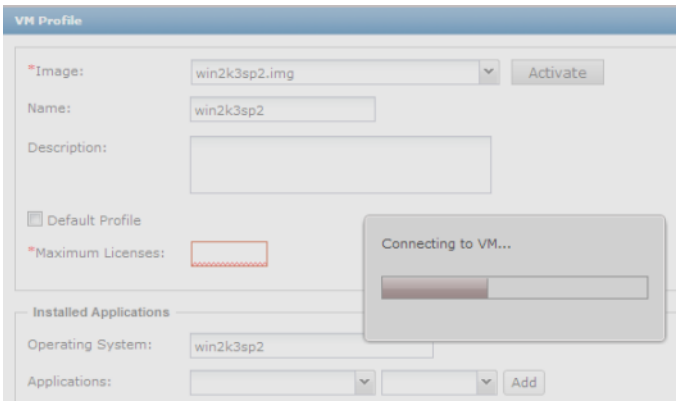



**Figure 5-8 Progress of the VM creation**

Based on your browser settings, warning messages are displayed before the VM starts.

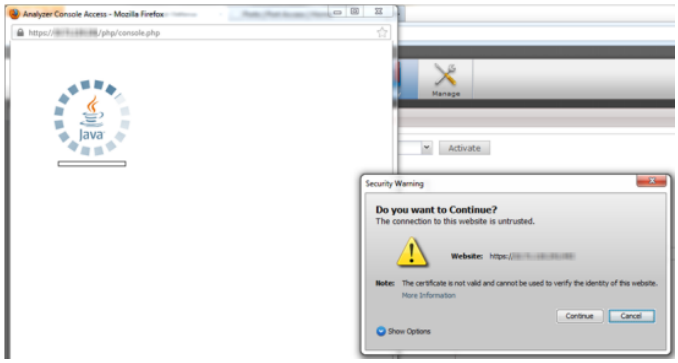



**Figure 5-9 Warning message**

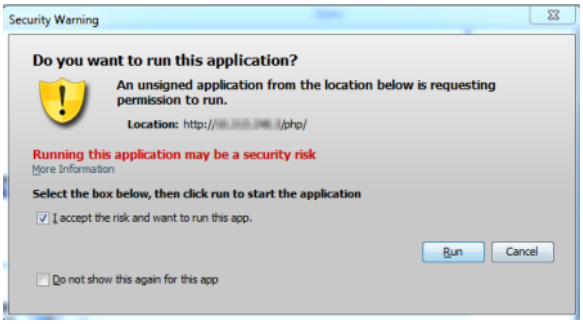

Security Warning
Do you want to run this application?
An unsigned application from the location below is requesting permission to run.
Location: http://
Running this application may be a security risk
More Information
Select the box below, then click run to start the application
I accept the risk and want to run this app.
Run
Cancel
Do not show this again for this app

**Figure 5-10 Warning message**

After you OK the warning messages, the VM starts.

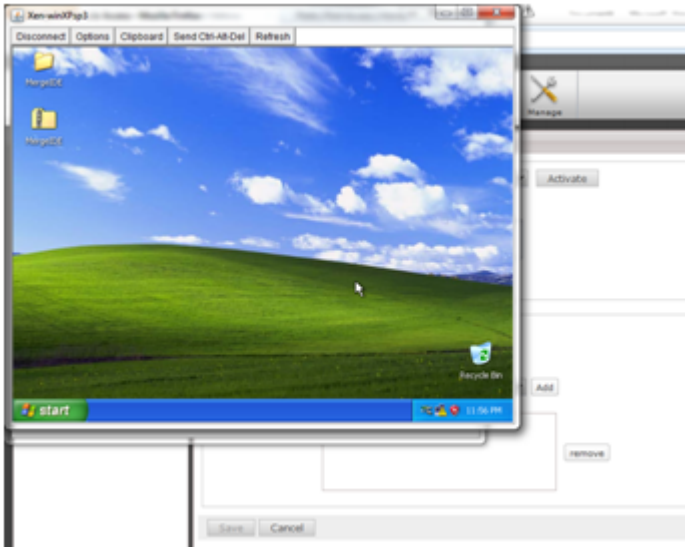



**Figure 5-11 VM displayed in a pop-up window**

4 After the VM is up, properly shut it down and close the pop-up window.

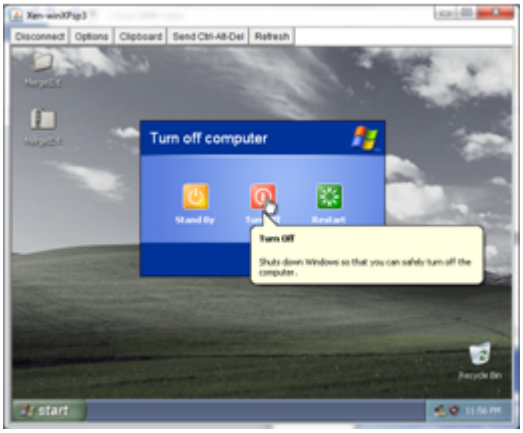



**Figure 5-12 Shut down the VM**

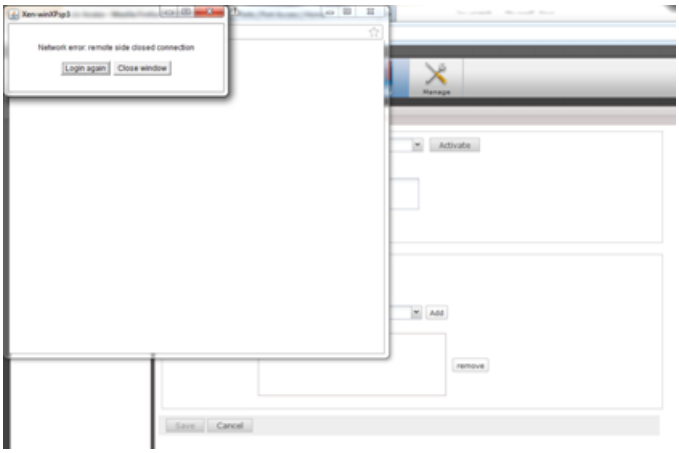



**Figure 5-13 Close the pop-up window**

5 Click **Validate**.

**Figure 5-14 Validating the image file**

McAfee Advanced Threat Defense ensures that the VM is adapted to the McAfee Advanced Threat Defense Appliance hardware. Also, it checks if the VM is working fine, configures the required networking details, checks the applications installed, and so on. If the VM is found to work fine, the validation is successful.

Click **Check Status** to view the image validation log. You can proceed to create the VM profile only if the validation is successful. If the validation fails, review the validation log for the reason. Then create a new VMDK with the correct settings and redo the process of creating the analyzer VM.

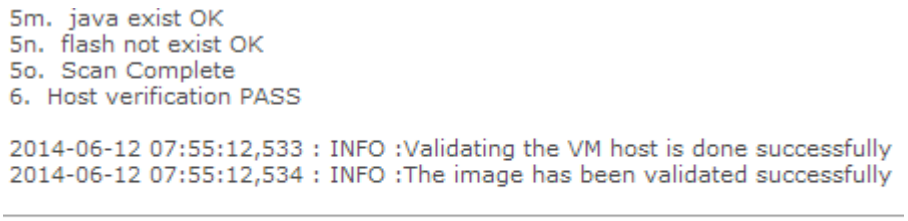

5m. java exist OK
5n. flash not exist OK
5o. Scan Complete
6. Host verification PASS
2014-06-12 07:55:12,533 : INFO :Validating the VM host is done successfully
2014-06-12 07:55:12,534 : INFO :The image has been validated successfully

**Figure 5-15 Image validation log**

6 Create the VM profile for the VM that you created by entering the appropriate information in the respective fields.

**Table 5-3 Option definitions**

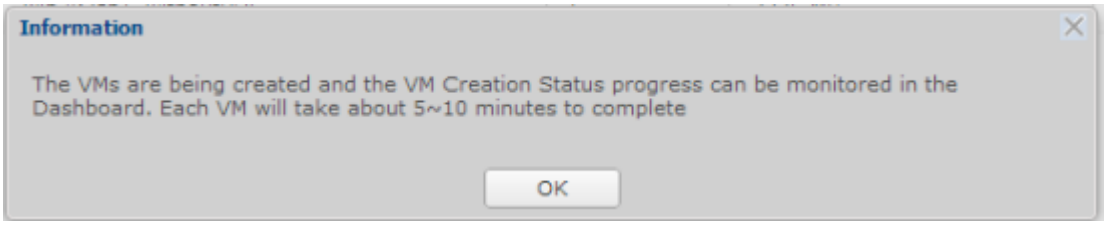
| Option name | Definition |
|---|---|
| **Name** | The name of the image file is automatically displayed as the name for the VM profile. You cannot modify it. |
| **Description** | Optionally, provide a detailed description of the VM profile. |

**Table 5-3 Option definitions** *(continued)*

| Option name | Definition |
|---|---|
| **Default Profile** | The first time, you must select it to make the VM profile the default one; subsequently you can select or ignore it.<br>For a file, if the target host environment is not available or if the required analyzer VM is not available, McAfee Advanced Threat Defense uses this VM to dynamically analyze the file. |
| **Maximum Licenses** | Enter the number of concurrent user licenses that you possess. You must factor in the operating system as well as the applications in the image file. Consider that the image file is a Windows 7 machine with Microsoft Office installed. You have 3 concurrent licenses for Windows 7 and 2 for Microsoft Office. In this case, you must enter 2 as the maximum licenses.<br>This is one of the factors that determine the number of concurrent analyzer VMs that McAfee Advanced Threat Defense creates from the image file.<br>The maximum analyzer VMs supported on an ATD-3000 is 30 and on an ATD-6000, it is 60. That is, the cumulative value of **Maximum Licenses** in all the VM profiles must not exceed 30 for an ATD-3000 and 60 for an ATD-6000, including the default Android analyzer VM. So, you can have up to 29 licenses for Windows analyzer VMs in an ATD-3000 and 59 in case of ATD-6000.<br>The maximum number of analyzer VMs that you can upload to a McAfee Advanced Threat Defense Appliance depends on the Windows operating system type as well as the Appliance type.<br>• Windows Server 2008, Windows Server 2003 SP1/SP2, Windows 7 SP1 64-bit, and Windows 7 SP1 32-bit: Up to 20 analyzer VMs on ATD-3000 and 40 on ATD-6000.<br>• Windows XP SP2/SP3: Up to 30 analyzer VMs on ATD-3000 and 60 on ATD-6000. |
| **Save** | Creates the VM profile record with the information you provided.<br>When you click **Save**, the VM creation starts in the background, running as a daemon, and the VM profile is listed in the VM Profile page.<br>Even if the newly created VM profile is listed in the **VM Profile** page, it might take 10-15 minutes before the analyzer VM and VM profile are ready for use. |
| **Cancel** | Closes the **VM Profile** page without saving the changes. |

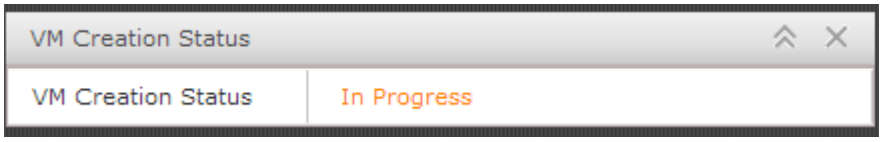
7 Monitor the progress of VM creation.

A message is displayed about the VM creation.


Information
The VMs are being created and the VM Creation Status progress can be monitored in the Dashboard. Each VM will take about 5~10 minutes to complete
OK

You can monitor the progress using the following methods:

- Select **Dashboard** and check the **VM Creation Status** monitor.



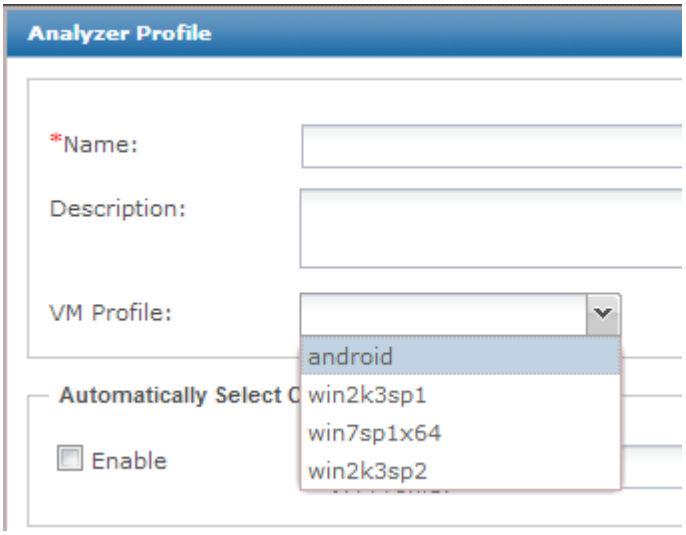

- Select **Policy** | **VM Profile** to view the status against the corresponding VM profile.




To view the system logs related to VM creation, select **Manage** | **System Log**. an

8 To confirm successful VM profile creation, select **Policy** | **Analyzer Profile** and check if the VM profile that you created is listed in the **VM Profile** drop-down.

**Figure 5-16**




# Edit VM profiles

**Before you begin**

To edit a VM profile, either you must have created it or you must have admin-user role.

## Task

1 Select **Policy** | **VM Profile**.

The currently available VM profiles are listed.

2 Select the required record and click **Edit**.

The **VM Profile** page is displayed.

3 Make the changes to the required fields and click **Save**.

## Delete VM profiles

**Before you begin**

- To delete a VM profile, either you must have created it or you must have admin-user role.
- Make sure the VM profile you want to delete is not specified in the analyzer profiles.

### Task

1 Select **Policy** | **VM Profile**.

The currently available VM profiles are displayed.

2 Select the required record and click **Delete**.

3 Click **Yes** to confirm deletion.

# View the VM creation log

When you create a VM profile using the **VM Profile** page, McAfee Advanced Threat Defense creates an analyzer VM from the image file you selected in the VM profile record. Simultaneously, it prints the related logs, which you can view in the McAfee Advanced Threat Defense web application. Through these log entries, you can view what is happening as the analyzer VM is being created. You can use this information for troubleshooting purposes.

### Task

- After you click **Save** in the **VM Profile** page, select **Manage** | **VM Creation Log** to view the log entries.

  You cannot print or export the log entries.

# 6 Configuring McAfee Advanced Threat Defense for malware analysis

After you install McAfee Advanced Threat Defense Appliance on your network, you can configure it to analyze malware. For this, you use the McAfee Advanced Threat Defense web application. You must have at least the web-access role to configure malware analysis.

This section introduces you to the related terminologies and provides the procedures to set up McAfee Advanced Threat Defense for malware analysis.

**Contents**


- *Terminologies*
- *High-level steps for configuring malware analysis*
- *How McAfee Advanced Threat Defense analyzes malware?*
- *Managing analyzer profiles*
- *Integration with McAfee ePO*
- *Specify proxy server for internet connectivity*
- *Configure the proxy DNS settings*
- *Configure date and time settings*
- *Define custom YARA rules for identifying malware*


## Terminologies

Being familiar with the following terminologies facilitates malware analysis using McAfee Advanced Threat Defense.

- **Static analysis** — When McAfee Advanced Threat Defense receives a supported file for analysis, it first performs static analysis of the file. The objective is to check if it is a known malware in the shortest possible time, and also to preserve the McAfee Advanced Threat Defense resources for dynamic

analysis. For static analysis, McAfee Advanced Threat Defense uses the following resources and in the same order:

- **Local whitelist —** This is the list of MD5 hash values of trusted files, which need not be analyzed. This whitelist is based on the McAfee® Application Control database that is used by other solutions in the McAfee suite. This has over 230,000,000 entries.

  The whitelist feature is enabled by default. To disable it, use the `setwhitelist` command. There are commands to manage the entries in the whitelist. The static McAfee® Application Control database cannot be modified. However, you can add or delete entries based on file hash. You can also query the whitelist for a certain file hash to see if it has been added to the database.

  The default whitelist entries are not periodically updated. However, they might be updated when you upgrade the McAfee Advanced Threat Defense software.

  The McAfee products that submit files to McAfee Advanced Threat Defense do have the capability to perform custom whitelisting as well. This includes the McAfee Web Gateway and the McAfee Network Security Platform

  See whitelist on page 319 for the commands.

- **Local blacklist —** This is the list of MD5 hash values of known malware stored in the McAfee Advanced Threat Defense database. When McAfee Advanced Threat Defense detects a malware through its heuristic McAfee Gateway Anti-Malware engine or through dynamic analysis, it updates the local blacklist with the file's MD5 hash value. A file is added to this list automatically only when its malware severity as determined by McAfee Advanced Threat Defense is medium, high, or very high. There are commands to manage the entries in the blacklist.

  See Blacklist on page 303 for the commands.

- **McAfee GTI —** This is a global threat correlation engine and intelligence base of global messaging and communication behavior, which enables the protection of the customers against both known and emerging electronic threats across all threat areas. The communication behavior includes the reputation, volume, and network traffic patterns. McAfee Advanced Threat Defense uses both the IP Reputation and File Reputation features of GTI.

  For File Reputation queries to succeed, make sure McAfee Advanced Threat Defense is able to communicate with `tunnel.message.trustedsource.org` over HTTPS (TCP/443). McAfee Advanced Threat Defense retrieves the URL updates from `List.smartfilter.com` over HTTP (TCP/80).

- **Gateway Anti-Malware —** McAfee Gateway Anti-Malware Engine analyzes the behavior of web sites, web site code, and downloaded Web 2.0 content in real time to preemptively detect and block malicious web attacks. It protects businesses from modern blended attacks, including viruses, worms, adware, spyware, riskware, and other crimeware threats, without relying on virus signatures.

  McAfee Gateway Anti-Malware Engine is embedded within McAfee Advanced Threat Defense to provide real-time malware detection.

- **Anti-Malware** — McAfee Anti-Malware Engine is embedded within McAfee Advanced Threat Defense. The DAT is updated either manually or automatically based on the network connectivity of McAfee Advanced Threat Defense.

  Static analysis also involves analysis through reverse engineering of the malicious code. This includes analyzing all the instructions and properties to identify the intended behaviors, which might not surface immediately. This also provides detailed malware classification information, widens the security cover, and can identify associated malware that leverages code re-use.

By default, McAfee Advanced Threat Defense downloads the updates for McAfee Gateway Anti-Malware Engine and McAfee Anti-Malware Engine every 90 minutes. To update immediately, use update_avdat on page 319 CLI command. For these updates to succeed, make sure McAfee Advanced Threat Defense can contact `wpm.webwasher.com` over HTTPS (TCP/443).

- **Dynamic analysis —** In this case, McAfee Advanced Threat Defense executes the file in a secure VM and monitors its behavior to check how malicious the file is. At the end of the analysis, it provides a detailed report as required by the user. McAfee Advanced Threat Defense does dynamic analysis after the static analysis is done. By default, if static analysis identifies the malware, McAfee Advanced Threat Defense does not perform dynamic analysis. However, you can configure McAfee Advanced Threat Defense to perform dynamic analysis regardless of the results from static analysis. You can also configure only dynamic analysis without static analysis. Dynamic analysis includes the disassembly listing feature of McAfee Advanced Threat Defense as well. This feature can generate the disassembly code of PE files for you to analyze the sample further.

- **Analyzer VM —** This is the virtual machine on the McAfee Advanced Threat Defense that is used for dynamic analysis. To create the analyzer VMs, you need to create the VMDK file with the required operating system and applications. Then, using SFTP, you import this file into the McAfee Advanced Threat Defense Appliance.

  Only the following operating systems are supported to create the analyzer VMs:

  - Microsoft Windows XP 32-bit Service Pack 2
  - Microsoft Windows XP 32-bit Service Pack 3
  - Microsoft Windows Server 2003 32-bit Service Pack 1
  - Microsoft Windows Server 2003 32-bit Service Pack 2
  - Microsoft Windows Server 2008 R2 Service Pack 1
  - Microsoft Windows 7 32-bit Service Pack 1
  - Microsoft Windows 7 64-bit Service Pack 1
  - Microsoft Windows 8.0 Pro 32-bit
  - Microsoft Windows 8.0 Pro 64-bit
  - Android 2.3 by default. You can upgrade it to Android 4.3. See Upgrade the Android analyzer VM on page 49.

All of the above Windows operating systems can be in English, Chinese Simplified, Japanese, German, or Italian.

The only pre-installed analyzer VM is the Android VM.

You must create analyzer VMs for Windows. You can create different VMs based on your requirements. The number of analyzer VMs that you can create is limited only by the disk space of the McAfee Advanced Threat Defense Appliance. However, there is a limit as to how many of them can be used concurrently for analysis. The number of concurrent licenses that you specify also affects the number of concurrent instances for an analyzer VM.

- **VM profile —** After you upload the VM image (.vmdk file) to McAfee Advanced Threat Defense, you associate each of them with a separate VM profile. A VM profile indicates what is installed in a VM image and the number of concurrent licenses associated with that VM image. Using the VM image and the information in the VM profile, McAfee Advanced Threat Defense creates the corresponding number of analyzer VMs. For example, if you specify that you have 10 licenses for Windows XP SP2 32-bit, then McAfee Advanced Threat Defense understands that it can create up to 10 concurrent VMs using the corresponding .vmdk file.
- **Analyzer profile —** This defines how to analyze a file and what to report. In an analyzer profile, you configure the following:
  - VM profile
  - Analysis options
  - Reports you wish to see after the analysis
  - Password for zipped sample files
  - Minimum and maximum execution time for dynamic analysis

  You can create multiple analyzer profiles based on your requirements. For each McAfee Advanced Threat Defense user, you must specify a default analyzer profile. This is the analyzer profile that is used for all files uploaded by the user. Users who use the McAfee Advanced Threat Defense web application to manually upload files for analysis, can choose a different analyzer profile at the time of file upload. Always, the analyzer profile selected for a file takes precedence over the default analyzer profile of the corresponding user.

  To dynamically analyze a file, the corresponding user must have the VM profile specified in the user's analyzer profile. This is how the user indicates the environment in which McAfee Advanced Threat Defense should execute the file. You can also specify a default Windows 32-bit and a 64-bit VM profile.
- **User —** A McAfee Advanced Threat Defense user is one who has the required permissions to submit files to McAfee Advanced Threat Defense for analysis and view the results. In case of manual submission, a user could use the McAfee Advanced Threat Defense web application or an FTP client. In case of automatic submission, you integrate McAfee products such as McAfee Network Security Platform or McAfee Web Gateway with McAfee Advanced Threat Defense. Then when these products detect a file download, they automatically submit the file to McAfee Advanced Threat Defense before allowing the download to complete. So, for these products default user profiles are available in McAfee Advanced Threat Defense.

  For each user, you define the default analyzer profile, which in turn can contain the VM profile. If you use the McAfee Advanced Threat Defense for uploading files for analysis, you can override this default profile at the time of file submission. For other users, McAfee Advanced Threat Defense uses the default profiles.

# High-level steps for configuring malware analysis

This section provides the high-level steps on how to configure McAfee Advanced Threat Defense for malware analysis and reporting:

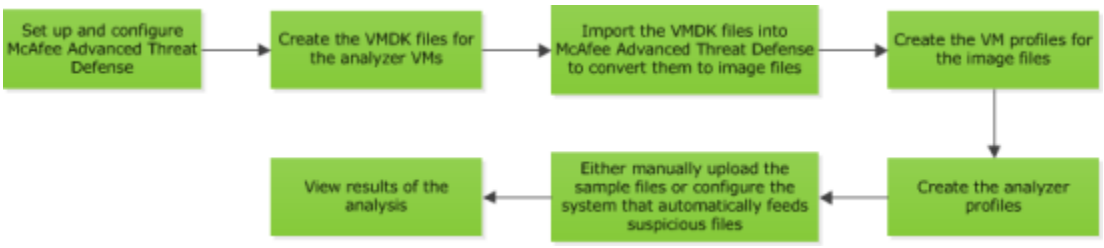

Set up and configure McAfee Advanced Threat Defense
Create the VMDK files for the analyzer VMs
Import the VMDK files into McAfee Advanced Threat Defense to convert them to image files
Create the VM profiles for the image files
Create the analyzer profiles
Either manually upload the sample files or configure the system that automatically feeds suspicious files
View results of the analysis

**Figure 6-1 Summarized steps for configuring malware analysis**

1 Set up the McAfee Advanced Threat Defense Appliance and ensure that it is up and running.

- Based on your deployment option, make sure the McAfee Advanced Threat Defense Appliance has the required network connections. For example, if you integrate it with Network Security Platform, make sure the Sensor, Manager, and the McAfee Advanced Threat Defense Appliance are able to communicate with each other.
- Make sure the required static analysis modules, such as the McAfee Gateway Anti-Malware Engine are up-to-date.

2 Create the analyzer VMs and the VM profiles. See Creating analyzer VM on page 4.

3 Create the analyzer profiles that you need. See Managing analyzer profiles on page 229.

4 If you want McAfee Advanced Threat Defense to upload the results to an FTP server, configure it and have the details with you before you create the profiles for the corresponding users.

5 Create the required user profiles. See Add users on page 37.

6 Log on to McAfee Advanced Threat Defense web application using the credentials of a user you created and upload a sample file for analysis. This is to check if you have configured McAfee Advanced Threat Defense as required. See Upload files for analysis using McAfee Advanced Threat Defense web application on page 248.

7 In the **Analysis Status** page, monitor the status of the analysis. See Monitor the status of malware analysis on page 257

8 After the analysis is complete, view the report in the **Analysis Results** page. See View the analysis results on page 259.

# How McAfee Advanced Threat Defense analyzes malware?

This section explains a typical workflow when McAfee Advanced Threat Defense analyzes files for malware.

Consider that you have uploaded a file manually using McAfee Advanced Threat Defense web application:

1 Assuming the file format is supported, McAfee Advanced Threat Defense unpacks the file and calculates the MD5 hash value.

2 McAfee Advanced Threat Defense applies the analyzer profile that you specified during file upload.

3 Based on the configuration in the analyzer profile, it determines the modules to use for static analysis and checks the file against those modules.

4 If the file is found to be malicious during static analysis, McAfee Advanced Threat Defense stops further analysis and generates the required reports. This, however, depends on how you have configured the corresponding analyzer profile.

5 If the static analysis does not report any malware or if you had configured McAfee Advanced Threat Defense to perform dynamic analysis regardless of the results from static analysis, McAfee Advanced Threat Defense initiates dynamic analysis for the file.

6 It executes the file in the corresponding analyzer VMs and records every behavior. The analyzer VM is determined based on the VM profile in the analyzer profile.

7 If the file is fully executed or if the maximum execution period expires, McAfee Advanced Threat Defense prepares the required reports.

8 After dynamic analysis is complete, it sets the analyzer VMs to their baseline version so that they can be used for the next file in queue.

## Internet access to sample files

When being dynamically analyzed, a sample might access a resource on the Internet. For example, the sample might attempt to download additional malicious code or attempt to upload information that it collected from the host machine (in this case, the analyzer VM). You can configure McAfee Advanced Threat Defense to provide network services to analyzer VMs so that the network activities of a sample file can be analyzed.

Providing Internet access to samples enables McAfee Advanced Threat Defense to analyze the network behavior of a sample and also determine the impact of the additional files downloaded from the Internet. Some malware might try to determine if they are being executed in a sandbox by requesting for Internet access and then alter their behavior accordingly.

When an analyzer VM is created, McAfee Advanced Threat Defense makes sure that the analyzer VM has the configurations to communicate over a network when required.

You can control granting real network access to an analyzer VM through a setting in the analyzer profiles. Network services are provided regardless of the method used to submit the sample. For example, it is provided to samples submitted manually using the McAfee Advanced Threat Defense web application as well as samples submitted by the integrated products.

The following is the high-level process flow when a sample accesses a resource on the Internet.

1 A sample attempts to access a resource on the Internet.

2 McAfee Advanced Threat Defense checks if the Internet connectivity is enabled in the corresponding analyzer profile used for this analysis.

3 Based on whether Internet connectivity is enabled or not, McAfee Advanced Threat Defense determines the mode in which network services are to be provided.

- Simulator mode — If Internet connectivity is not enabled in the analyzer profile, this mode is used. McAfee Advanced Threat Defense can represent itself as being the target resource. For example, if the sample attempts to download a file through FTP, McAfee Advanced Threat Defense simulates this connection for the analyzer VM.
- Real Internet mode — This mode requires the management port (eth-0), eth-1, eth-2 or eth-3 to have access to the Internet. If Internet connectivity is enabled in the analyzer profile, McAfee Advanced Threat Defense uses this mode. McAfee Advanced Threat Defense provides real Internet connection through the management port by default, which is publicly routed or directed towards your enterprise firewall as per your network configuration. Because the traffic from an analyzer VM could be malicious, you might want to segregate this traffic away from your production network. In this case, you can use McAfee Advanced Threat Defense's eth-1, eth-2, or eth-3 provide Internet access to the analyzer VM.

Even if you have configured a HTTP proxy server in the **HTTP Proxy Settings** page, this traffic is not routed to that server. So, make sure your enterprise firewall is configured to handle this traffic.

4 Regardless of the mode used, McAfee Advanced Threat Defense logs all the network activities. However, the types of reports generated might vary based on the mode.

- Network activities are summarized and presented in the Analysis Summary report. You can find the DNS queries and socket activities under network operations. You can find all the network activities in the **Network Simulator** section of the report.
- The dns.log report also contains the DNS queries made by the sample.
- The packet capture of the network activities is provided in the NetLog folder within the Complete Results zip file.

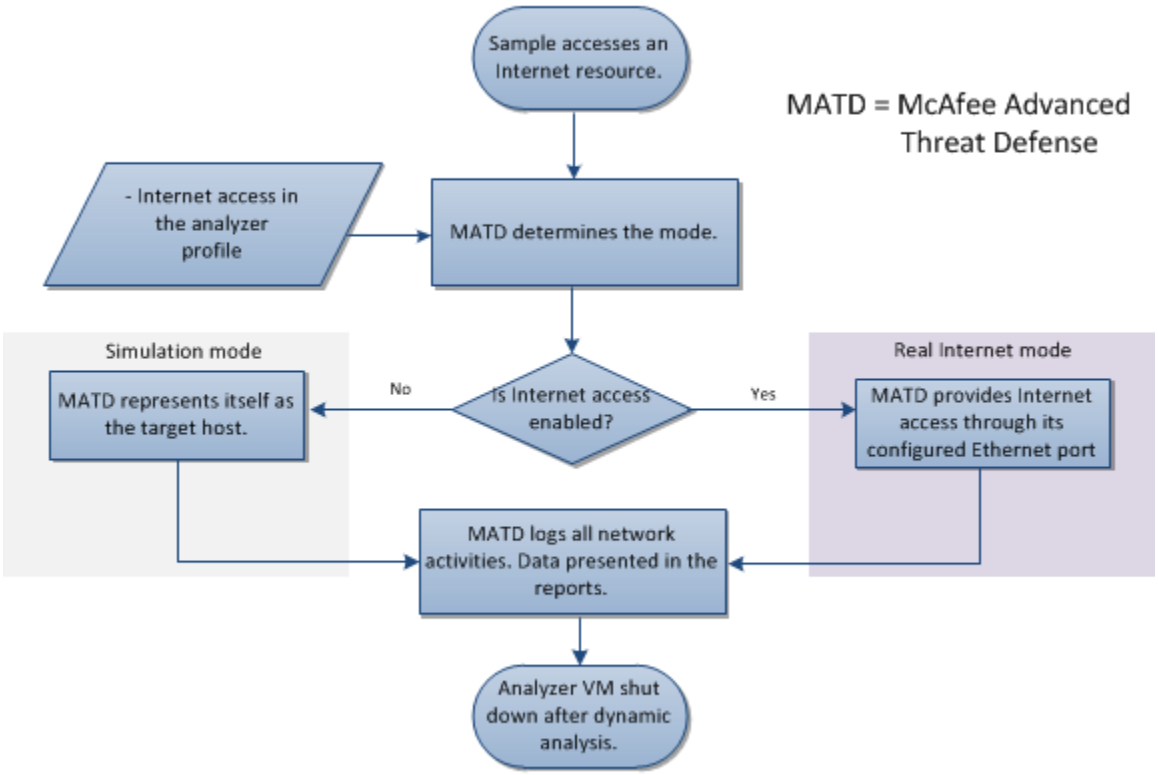

Sample accesses an Internet resource.
MATD = McAfee Advanced Threat Defense
- Internet access in the analyzer profile
MATD determines the mode.
Simulation mode
MATD represents itself as the target host.
No
Is Internet access enabled?
Yes
Real Internet mode
MATD provides Internet access through its configured Ethernet port
MATD logs all network activities. Data presented in the reports.
Analyzer VM shut down after dynamic analysis.

**Figure 6-2 Internet access to samples - process flow**

Recall that McAfee Advanced Threat Defense uses its management port (eth-0) by default to provide Internet access to samples. You can also configure a different port for this purpose.

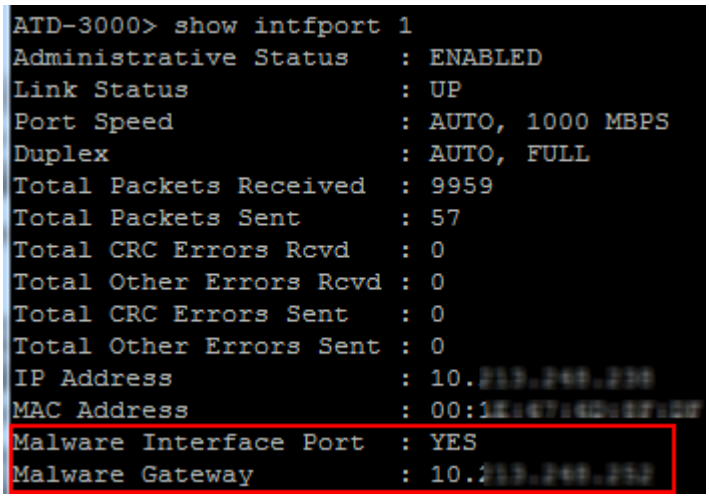
To enable a different Ethernet port for malware network access, follow the procedure below:

1 Log on to the McAfee Advanced Threat Defense CLI and enable the required port. For example, `set intfport 1 enable` to enable eth-1 port.

2 Set the required IP address and subnet mask for the port. For example, `set intfport 1 10.10.10.10 255.255.255.0`

3 For the Ethernet port, set the gateway through which you want to route the Internet access. For example, `set malware-intfport 1 gateway 10.10.10.252`

4 Run the `show intfport <port number>` command for the port to check if it is configured for malware Internet access. For example, `show intfport 1`. Verify the `Malware Interface Port` and `Malware Gateway` entries.


ATD-3000> show intfport 1
Administrative Status : ENABLED
Link Status : UP
Port Speed : AUTO, 1000 MBPS
Duplex : AUTO, FULL
Total Packets Received : 9959
Total Packets Sent : 57
Total CRC Errors Rcvd : 0
Total Other Errors Rcvd : 0
Total CRC Errors Sent : 0
Total Other Errors Sent : 0
IP Address : 10.
MAC Address : 00:
Malware Interface Port : YES
Malware Gateway : 10.

- To revert to the managment port (eth-0) for malware Internet access, run `set malware-intfport mgmt` in the CLI. McAfee Advanced Threat Defense uses its management port IP and the corresponding default gateway to provide Internet access to samples.
- Suppose you configured eth-1 for malware Internet access but now you want to use eth-2. Then, follow the above procedure for eth-2. Eth-2 is set as the port for Internet access for malware.
- Suppose you configured eth-1 for Internet access but now you want to use eth-1 but with a different IP address or gateway. Then, repeat the procedure but with the new IP address or gateway.
- The `route add network` command is for general Advanced Threat Defense traffic. Whereas, `set malware-intfport` is for Internet traffic from an analyzer VM. So, the `route add network` and the `set malware-intfport` commands do not affect each other.

# Managing analyzer profiles

When a file is manually or automatically submitted to McAfee Advanced Threat Defense for analysis, it uses the corresponding analyzer profile to determine how the file needs to be analyzed and what needs to be reported in the analysis results. You specify the VM profile in the analyzer profile. You also define how the file is to be analyzed for malware and the reports to be published. Thus, an analyzer profile contains all the critical user-configuration on how to analyze a file.

You use the McAfee Advanced Threat Defense web application to manage analyzer profiles.

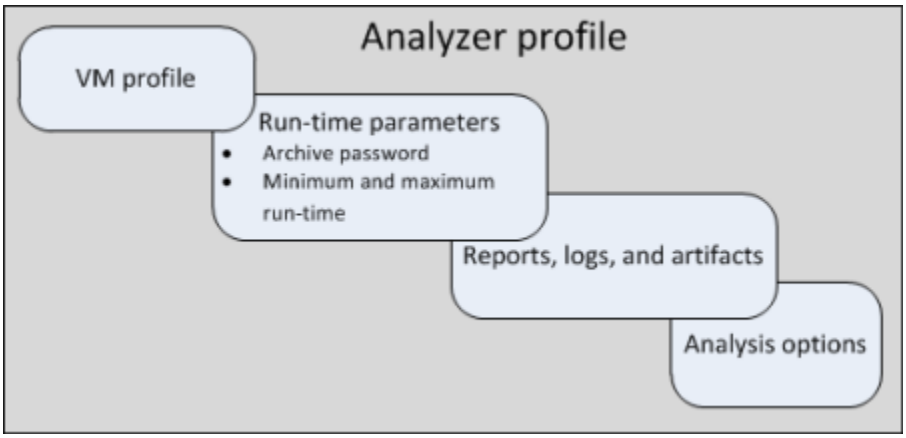



**Figure 6-3 Contents of an analyzer profile**

## View analyzer profiles

Based on your user role, you can view the existing analyzer profiles in the McAfee Advanced Threat Defense web application.

### Task

1 Select **Policy** | **Analyzer Profile**.

If you have web access, you can view only the analyzer profiles that you created. If you have admin access, you can view all the analyzer profiles currently in the database.

| Column name | Definition |
|---|---|
| **Select** | Select to edit or delete the corresponding analyzer profile. |
| **Name** | Name that you have assigned to the analyzer profile. |
| **Description** | The description of the characteristics of the analyzer profile. |
| **OS Name** | Corresponds to the name of the VM profile specified in the analyzer profile. |
| **Automatically Select OS** | Indicates if you have selected the **Automatically Select OS** option in the analyzer profile. |

2 Hide the unneeded columns.

a Move the mouse over the right corner of a column heading and click the drop-down arrow.

b Select **Columns**.

c Select only the required column names from the list.

You can click a column heading and drag it to the required position.

3 To sort the records based on a particular column name, click the column heading.

You can sort the records in the ascending or descending order. Alternatively, move the mouse over the right corner of a column heading and click the drop-down arrow. Then select **Sort Ascending** or **Sort Descending**.

4 To view the complete details of a specific analyzer profile, select the record and click **View**.

# Create analyzer profiles

**Before you begin**

- If you intend to select the dynamic analysis option in the analyzer profile, make sure that you have created the required VM profile. VM profiles are also required if you want to use the **Automatically Select OS** option.
- If you want to enable Internet access to samples, then you need admin user privileges.

## Task

1 Select **Policy** | **Analyzer Profile** | **New**.

The **Analyzer Profile** page is displayed.

2 Enter the appropriate information in the respective fields.

| Option name | Definition |
|---|---|
| **Name** | Enter the name for the analyzer profile. It should allow you to easily identify the characteristics of that analyzer profile. |
| **Description** | Optionally, provide a detailed description of the analyzer profile. |
| **VM Profile** | Select the VM profile McAfee Advanced Threat Defense must use for dynamically analyzing a file. |
| **Automatically Select OS** | If you want McAfee Advanced Threat Defense to automatically select the VM profile for Windows 32 bit and Windows 64 bit, select **Enable** and then select the VM profiles from the **Windows 32-bit VM Profile** and **Windows 64-bit VM Profile**.<br>Consider that for **VM Profile**, you have selected Android. You have enabled **Automatically Select OS**. For **Windows 32-bit VM Profile**, you have selected Windows XP SP3 and for **Windows 64-bit VM Profile**, you have selected Windows 7 SP1 64-bit.<br>Now, when an .apk file is detected, the Android analyzer VM is used for dynamically analyzing the file. Similarly, for a PE32 file, Windows XP SP3 is used. For a PE64 file, Windows 7 SP1 64-bit analyzer VM is used.<br>If McAfee Advanced Threat Defense is unable to determine the operating system for this analyzer profile or if the determined analyzer VM is not available, it uses the VM mentioned in the **VM Profile** field. |
| **Archive Password** | Enter the password for McAfee Advanced Threat Defense to unzip a password-protected malware sample. |
| **Confirm Password** | Re-enter the password for confirmation. |
| **Minimum Run Time (sec)** | Specify the minimum time duration for which McAfee Advanced Threat Defense should dynamically analyze the sample. The default value is 5 seconds. The maximum value allowed is 600 seconds. If the file stops executing before this time period, dynamic analysis is stopped. |
| **Maximum Run Time (sec)** | Specify the maximum time duration for which McAfee Advanced Threat Defense should dynamically analyze the sample. The default value is 180 seconds. The maximum value allowed is 600 seconds. If the file does not stop execution before this time period expires, the dynamic analysis is stopped. |
| **Analysis Summary** | Select to include the Analysis Summary report in the analysis results. See View the Analysis Summary report on page 261. |
| **Packet captures** | Select to capture the network packets if the file attempts to communicate during dynamic analysis. The pcap file is provided in the complete results zip file. |
| **Dropped Files** | Select to generate the Files Created in Sandbox report. See Dropped files report on page 267. |
| **Disassembly Results** | Select if you want McAfee Advanced Threat Defense to generate the disassembly code of PE files. See Disassembly Results on page 267. |
| **Logic Path Graph** | Select to generate Logic Path Graph report. See Logic Path Graph on page 268. |
| **User API Log** | This report provides Windows user-level DLL API calls made directly by the malware sample during dynamic analysis. See User API Log on page 273. |
| **Local Black List** | Select if you want McAfee Advanced Threat Defense to check the file's MD5 hash value with the list of black-listed MD5 hash values in its local database. |
| **Anti-Malware** | Select if you want McAfee Advanced Threat Defense to scan the file using McAfee Anti-Malware Engine. |
| **GTI File Reputation** | Select if you want McAfee Advanced Threat Defense to check the file's MD5 hash value with McAfee GTI. Make sure McAfee Advanced Threat Defense is able to communicate with McAfee GTI, which is on the cloud. |
| **Gateway Anti-Malware** | Select if you want McAfee Advanced Threat Defense to check the file using McAfee Gateway Anti-Malware Engine. |

| Option name | Definition |
|---|---|
| **Sandbox** | Select if you want the file to be dynamically analyzed. A file is not dynamically analyzed if any of the static methods report it as a malware or a white-listed file. If you want to dynamically analyze the file regardless of the result from static analysis, select **Run All Selected** as well.<br>Make sure you have selected the VM profile and the **Runtime Parameters**. |
| **Run All Selected** | Select if you want McAfee Advanced Threat Defense to analyze the file using all the selected analyze options regardless of the result from any specific method. |
| **Enable Malware Internet Access** | Select to provide Internet access to samples when they attempt to access a resource on the Internet.<br>To enable this option, the **Sandbox** option under Analyzer Options must be enabled. Also, you must have admin role privileges to select or deselect **Enable Malware Internet Access**.<br>Because the sample being analyzed could potentially be a malware, selecting the **Enable Malware Internet Access** option involves the risk of malicious traffic propagating out of your network. A disclaimer message is displayed when you select this option, and you must click **OK** to proceed. |
| **Save** | Creates the analyzer profile record with the information you provided. |
| **Cancel** | Closes the **Analyzer Profile** page without saving the changes. |

# Edit analyzer profiles

## Task

1 Select **Policy** | **Analyzer Profile**.

If you have web access, you can view only the analyzer profiles that you created. If you have admin access, you can view all the analyzer profiles currently in the database.

2 Select the required record and click **Edit**.

The **Analyzer Profile** page is displayed.

3 Make the changes to the required fields and click **Save**.

The changes affect the corresponding users even if they are currently logged on.

# Delete analyzer profiles

**Before you begin**

Make sure the users to whom you have assigned this analyzer profile are not currently logged on to McAfee Advanced Threat Defense.

## Task

1 Select **Policy** | **Analyzer Profile**.

If you have web access, you can view only the analyzer profiles that you created. If you have admin access, you can view all the analyzer profiles currently in the database.

2 Select the required record and click **Delete**.

3 Click **Yes** to confirm deletion.

# Integration with McAfee ePO

Integrating McAfee Advanced Threat Defense and McAfee ePO enables McAfee Advanced Threat Defense to correctly identify the target host environment and use the corresponding analyzer VM for dynamic analysis.

To determine the analyzer VM for a file submitted by Network Security Platform or McAfee Web Gateway, McAfee Advanced Threat Defense uses the following sources of information in the same order of priority:

1. McAfee Advanced Threat Defense queries McAfee ePO for the operating system of a host based on its IP address. If information from this source or if the corresponding analyzer VM is not available, it goes to the next source.
2. If Device Profiling is enabled, the Sensor provides the operating system and application details when forwarding a file for analysis. If information from this source or if the corresponding analyzer VM is not available, it goes to the next source.
3. From the analyzer profile in the corresponding user record, McAfee Advanced Threat Defense determines the VM profile. If information from this source or if the corresponding analyzer VM is not available, it goes to the next source.
4. The VM profile that you selected as the default. From the VM profiles in your setup, you can select one of them as the default one.

When McAfee Advanced Threat Defense receives host information for a particular IP address from McAfee ePO, it caches this detail.

- The cached IP address to host information data has a time to live (TTL) value of 48 hours.
- For the first 24 hours, McAfee Advanced Threat Defense just uses the host information in the cache.
- For the second 24 hours, that is from 24 to 48 hours, McAfee Advanced Threat Defense uses the host information from the cache but also queries McAfee ePO and updates its cache. This updated information is valid for the next 48 hours.
- If the cached information is more than 48 hours old, it treats it as if there is no cached information for the corresponding IP address. That is, it attempts to find the information from other sources and also sends a query to McAfee ePO.

The following explains how McAfee Advanced Threat Defense collaborates with McAfee ePO.

1. Network Security Platform or McAfee Web Gateway sends a file to McAfee Advanced Threat Defense for analysis. When Network Security Platform sends a file, the IP address of the target host is also sent.
2. McAfee Advanced Threat Defense checks its cache to see if there is a valid operating system mapped to that IP address.
3. If it is the first time that a file for that IP address is being analyzed, there is no information in the cache. So, it determines the analyzer VM from the device profiling information in case of Network Security Platform and user record in case of McAfee Web Gateway. Simultaneously, it sends a query to McAfee ePO for host information based on the IP address.
4. McAfee ePO forwards the host information to McAfee Advanced Threat Defense, which is cached for further use.

## Configure McAfee ePO integration

Integration with McAfee ePO, enables McAfee ePO to gather information such as the operating system and browsers installed on the target host. McAfee Advanced Threat Defense uses this information to select the best analyzer VM for dynamic analysis.

### Task

1 Select **Manage** | **ePO Login**.

The **ePO Login** page displays.

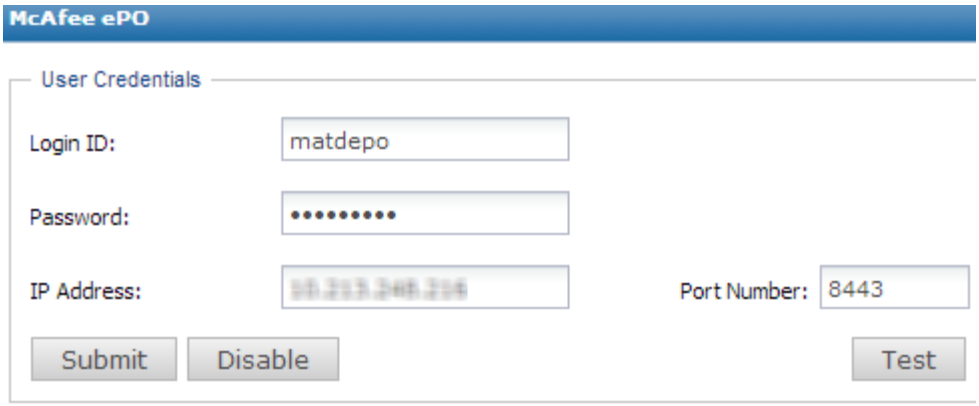



**Figure 6-4 McAfee ePO integration**

2 Enter the details in the appropriate fields.

| Option name | Definition |
|---|---|
| **Login ID** | Enter the McAfee ePO login name that McAfee Advanced Threat Defense should use to access the McAfee ePO server.<br>McAfee recommends you create a McAfee ePO user account with View-only permissions required for integration. |
| **Password** | Enter the password corresponding to the **Login ID** you entered. |
| **IP Address** | Enter the IPv4 address of the McAfee ePO server.<br>Contact your McAfee ePO administrator for the IP address. |
| **Port Number** | Specify the HTTPS listening port on the McAfee ePO server that will be used for the McAfee Advanced Threat Defense — McAfee ePO communication.<br>Contact your McAfee ePO administrator for the port number. |
| **Test** | Click to verify if McAfee Advanced Threat Defense is able to reach the configured McAfee ePO server over the specified port. |
| **Submit** | Click to save the configuration and enable McAfee Advanced Threat Defense — McAfee ePO integration. Make sure that the test connection is successful before you click **Save**. |
| **Disable** | Click to disable the integration between McAfee Advanced Threat Defense and McAfee ePO. |

# Specify proxy server for internet connectivity

If McAfee Advanced Threat Defense connects to a proxy server for internet connectivity, you can configure McAfee Advanced Threat Defense to connect to that server for proxy service.

### Task

1 Select **Manage** | **HTTP Proxy Setting**.

The **HTTP Proxy Setting** page is displayed.

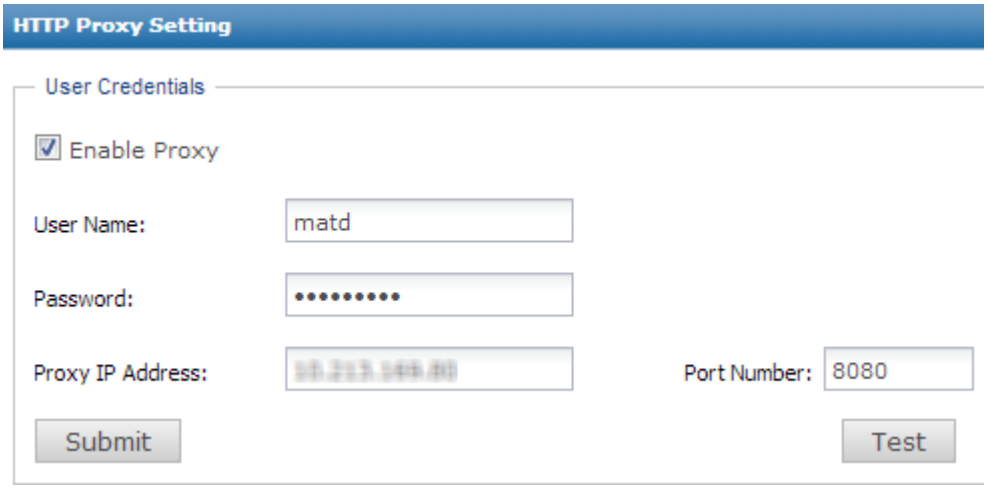



**Figure 6-5 Proxy Setting page**

2 Enter the appropriate information in the respective fields.

| Option name | Definition |
|---|---|
| **Enable Proxy** | Select to connect McAfee Advanced Threat Defense to a proxy server for Internet connectivity. |
| **User Name** | Enter the user name that McAfee Advanced Threat Defense for the proxied Internet connection. |
| **Password** | Enter the corresponding password. |
| **Proxy IP Address** | Enter the IPv4 address of the proxy server. |
| **Port Number** | Enter the port number on which the proxy server is listening for incoming connections. |
| **Test** | Click to verify if McAfee Advanced Threat Defense is able to reach the configured HTTP proxy server over the specified port. |
| **Submit** | Click to save the proxy settings in the database. Make sure that the test connection is successful before you click **Save**. |

# Configure the proxy DNS settings

When being executed, some files might send DNS queries to resolve names. Mostly, such queries are an attempt by malware to determine if they are being run in a sandbox environment. If the DNS query fails, the file might take an alternate path. When McAfee Advanced Threat Defense dynamically analyzes such a file, you might want to provide a proxy DNS service in order to bring out the actual behavior of the file.

### Task

1 Select **Manage** | **DNS Proxy Setting**.

The **DNS Proxy Setting** page is displayed.

2 Enter the appropriate information in the respective fields.

| Option name | Definition |
|---|---|
| **Domain** | Enter the Active Directory domain name, for example, McAfee.com. |
| **Preferred DNS Server** | Enter the IPv4 address of the primary DNS proxy server. The DNS queries from analyzer VMs are come to this DNS server. |
| **Alternate DNS Server** | Enter the IPv4 address of the secondary DNS proxy server. If the analyzer VM is unable to reach the primary DNS server, the DNS queries come to the secondary DNS server. |
| **Test** | Click verify if McAfee Advanced Threat Defense is able to reach either the preferred or the alternate DNS server. |
| **Submit** | Click to save the configuration in the database. Make sure that the test connection is successful before you click **Save**. |

# Configure date and time settings

**Before you begin**

- You need *admin user* privileges to view or set the date and time settings.
- If you plan to use domain names of Network Security Protocol (NTP) servers, make sure you have configured the DNS servers correctly in McAfee Advanced Threat Defense.

You can set the date and time on the McAfee Advanced Threat Defense Appliance as per your requirement in the **Date and Time Settings** page. McAfee Advanced Threat Defense uses the date and time that you configure for all its functional and display purposes. The date and time in the McAfee Advanced Threat Defense web application user interfaces, reports, log files, and CLI are all as per the date and time that you specify. For example, the timestamp in the Analysis Status and Analysis Results pages are as per the date and time that you configure.

You can either manually specify the date and time or configure Network Time Protocol (NTP) servers as the time source for McAfee Advanced Threat Defense. If you specify NTP servers, you can configure up to 3 Network Time Protocol (NTP) servers. In this case, McAfee Advanced Threat Defense acts as an NTP client and synchronizes with the highest priority NTP server that is available.

- By default, synchronization with NTP servers is enabled in McAfee Advanced Threat Defense. Also, `pool.ntp.org` is configured as the default NTP server. The default time zone is Pacific Standard Time (UTC-8).
- When you upgrade from a previous version without selecting the **Reset Database** option, the date and time settings from the previously installed version are preserved. If you upgrade with the **Reset Database** option selected, the default date and time settings as described above are set.
- At any point in time, there must be at least one valid NTP server specified in the **Date and Time Settings** page of McAfee Advanced Threat Defense. You can add, edit, or delete the list of NTP servers specified in McAfee Advanced Threat Defense.
- Based on the access available to McAfee Advanced Threat Defense, you can specify public NTP servers or the ones locally on your network.
- You can specify the domain name or the IPv4 address of NTP servers. If you specify the domain names, then you must have configured DNS settings in McAfee Advanced Threat Defense.

If you specify public NTP servers, then using the domain names instead of IP addresses is recommended. The domain of a public NTP server might resolve to different IP addresses based on various factors.

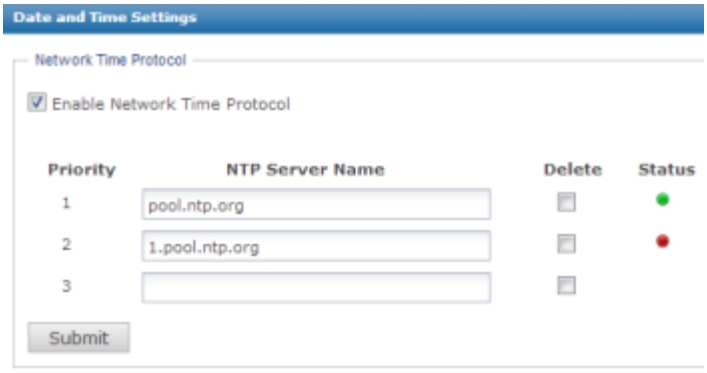
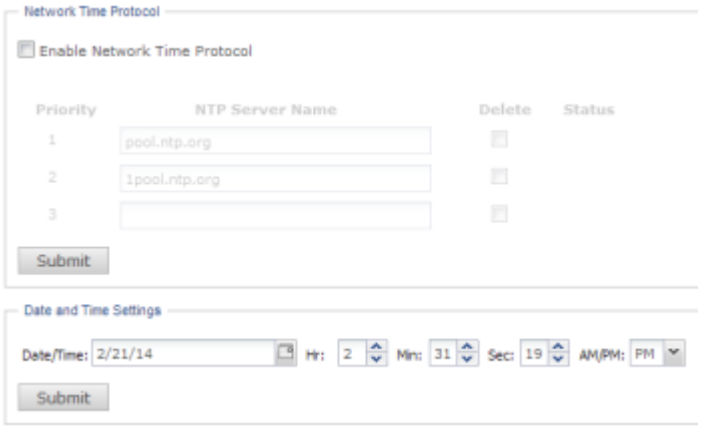
- Whether you enable NTP server synchronization or manually set the date and time, you must select the required time zone in the **Date and Time Settings** page. If you configure an NTP server, McAfee Advanced Threat Defense considers only the date and time from the NTP server. But for the time zone, it relies on what is specified in the Date and Time Settings page.
- 
- The date and time on a McAfee Advanced Threat Defense client has no impact on the timestamps that are displayed. Consider that the current time on the McAfee Advanced Threat Defense Appliance is 10 am PST (UTC-8). Regardless of the time zone from which you access this McAfee Advanced Threat Defense Appliance, all the timestamps are displayed in PST only. That is, the timestamps are not converted based on a client's date and time.
- When the current date and time settings are changed, the timestamp for all the older records are also changed accordingly. Consider that the current time zone is PST (UTC-8) and you change it to Japan Standard Time (UTC+9). Then the timestamp for the older records are all converted as per Japan Standard Time (JST). For example, if the timestamp displayed for a record in the **Analysis Status** page was 0100 hours (1 am) PST before you changed the time zone. After you change the time zone to JST, the timestamp for the same record is 1800 hours JST.
- The date and time settings of all the analyzer VMs are immediately synchronized to the date and time on the McAfee Advanced Threat Defense Appliance.

## Task

1 Select **Manage** | **Date and Time Settings**.

The **Date and Time Settings** page is displayed.

2 Enter the appropriate information in the respective fields and click **Submit** in the affected sections separately.

| Option name | Definition |
|---|---|
| **Enable Network Time Protocol** | Select if you want McAfee Advanced Threat Defense to act as an NTP client. By default this is selected.<br>To manually set the time for McAfee Advanced Threat Defense, deselect this option. |
| **Priority** | This is the order of priority assigned to the NTP servers. At the scheduled interval, McAfee Advanced Threat Defense attempts to synchronize with the first NTP server. If not available, it attempts to synchronize with the second and then the third. |
| **NTP Server Name** | Specify the domain name or IPv4 addresses of the NTP servers in the order of priority that McAfee Advanced Threat Defense should synchronize with. If you enter domain names, make sure you have configured the DNS settings properly.<br>At any point in time, there must be at least one reachable NTP server configured. |
| **Delete** | Select if you want to remove an NTP server from the list. |
| **Status** | Indicates whether a particular NTP server is reachable or not. Green indicates the server is reachable and red indicates that the server is not reachable.<br>  |
| **Date/Time** | To manually specify the date and time for McAfee Advanced Threat Defense, deselect **Enable Network Time Protocol** and click **Submit** under **Network Time Protocol**. Specify the date and time in the corresponding fields and then click **Submit** under **Date and Time Settings**.<br>  |

| Option name | Definition |
|---|---|
| **Select Time-zone** | Select the required time zone from the list and click **Submit** under **Time-zone Setting.** The default time zone is Pacific Time. |
| **Submit** | Implements the changes that you made in the corresponding sections of the **Date and time settings** page and also saves them in the database.<br>After you click **Submit** for Network Time Protocol, a success message is displayed. If you click **OK** for this message, McAfee Advanced Threat Defense checks if it can reach the specified NTP servers and updates the **Status** accordingly for each NTP server.<br> <br>You must click the **Submit** separately for affected sections. For example, if you make changes to the list of NTP servers and also change the time zone, you must click **Submit** under **Network Time Protocol** and **Submit** under **Time-zone Setting** separately. |

# Define custom YARA rules for identifying malware

YARA is a rule-based tool to identify and classify malware. McAfee Advanced Threat Defense enables you to use your own YARA rules to identify and classify malware. You can therefore import your own descriptions of malware into McAfee Advanced Threat Defense. YARA rules also enable you to customize the detection capabilities of McAfee Advanced Threat Defense to suit your needs. For example, you can use YARA rules if you would like certain registry operations to be reported as a particular severity level rather than the default severity level assigned by McAfee Advanced Threat Defense. You can also write YARA rules to catch zero-day or near-zero-day malware. You can write your own YARA rules or use the YARA rules from a third party.

In this section, the word sample, refers to both files and URLs that have been submitted to McAfee Advanced Threat Defense for malware analysis.

You can store your custom YARA rules in a text file. You can name this file such that it enables you track modifications to your YARA rule set. You import this text file into McAfee Advanced Threat Defense through the web application user interface. Internally, these rules are saved in a file named `custom.yara`.

Assuming you have enabled all analyze options with custom YARA rules, McAfee Advanced Threat Defense processes the sample files and URLs in the following order of priority:

1. Local whitelist
2. Local blacklist
3. McAfee GTI
4. McAfee Gateway Anti-Malware Engine
5. McAfee Anti-Malware Engine
6. Dynamic analysis

7 Custom YARA rules: These are user-managed YARA rules.

8 Internal YARA rules: These are internal YARA rules which are defined by McAfee and updated only during McAfee Advanced Threat Defense software upgrades, if necessary. You cannot view or download these rules.

McAfee Advanced Threat Defense checks a sample against YARA rules only if the sample is dynamically analyzed.

```
rule process_inject
{
meta:
Classification = 32
Description = "Changed access protection of pages to RW/RWE and injected into"
Severity = 4

strings:
$ntget =/(Nt|Zw)GetProcessHeap:/
$ntquery =/(Nt|Zw)QuerySystemInformation(Process|Thread):/
$ntopen =/(Nt|Zw)OpenProcess:/
$ntalloc =/(Nt|Zw)AllocateVirtualMemory:/
$ntwrite =/(Nt|Zw)WriteVirtualMemory:[0-9A-F ]{6,12}\([0-6]{1}[0-9A-E]{2,4},/
$service =/(svchost|csrss|lsass|spoolsv|services|winlogon|explorer|iexplore|winsvc)\.exe/ nocase

condition:
all of them
and
(for any i in (1..#ntquery) : (@ntopen > @ntquery[i])) //sequence of query/open
and
(for any i in (1..#ntopen) : (@service > @ntopen[i])) //service name for NtOpenProcess
}
```

**Figure 6-6 A sample YARA rule**

After you import your YARA rules into McAfee Advanced Threat Defense, the malware detection and classification are based on these rules as well. Final severity result of sample analysis is determined as a maximum value from analysis methods mentioned above, including custom YARA rules.

Down Selector's Analysis:

| Engine | GTI File Reputation | Gateway Anti-Malware | Anti-Malware | Custom Yara | Sandbox | Final |
|---|---|---|---|---|---|---|
| Threat Name | --- | --- | --- | --- | --- | |
| Severity | None | None | None | 4 | 2 | 4 |

This sample is malicious: final severity level 4

**Figure 6-7 Final score influenced by custom YARA rule score**

## Considerations

- McAfee Advanced Threat Defense supports custom YARA rules only from McAfee Advanced Threat Defense release 3.2.0.
- McAfee Advanced Threat Defense 3.2.0 supports YARA version 1.0 only. So, all YARA features documented in YARA User's Manual for version 1.0 are supported.

- In an McAfee Advanced Threat Defense cluster setup, each node maintains its set of custom YARA rules separately. That is, the custom YARA rules that you define in the primary node are not sent to the secondary nodes automatically.
- There is no limit on the number of rules that you can include in your custom YARA rules file. Neither is there a limit on the size of this file. However, the number of rules and their complexity might affect the performance of McAfee Advanced Threat Defense.

## Create the custom YARA rules file

**Before you begin**

- You are familiar with all features of YARA that McAfee Advanced Threat Defense currently supports.
- You have identified the user API log of the sample that you want to use as a reference for creating your YARA rules.

McAfee Advanced Threat Defense applies the custom YARA rules on the User API log of an analyzed sample. So, to create custom YARA rules to catch a specific behavior, you can use the user API log of a sample that caused the same behavior. You can use YARA rules to catch runtime DLLs, file operations, registry operations, process operations, and other operations reported in analysis summary report for a sample. For example, to catch a specific runtime DLL, see a sample's user API log and write a YARA rule for that DLL.

### Task

1 Create a text file and open it in a text editor such as Windows Notepad.

2 Enter the comments in the text file to track the APIs or data that are the sources for your YARA rules.

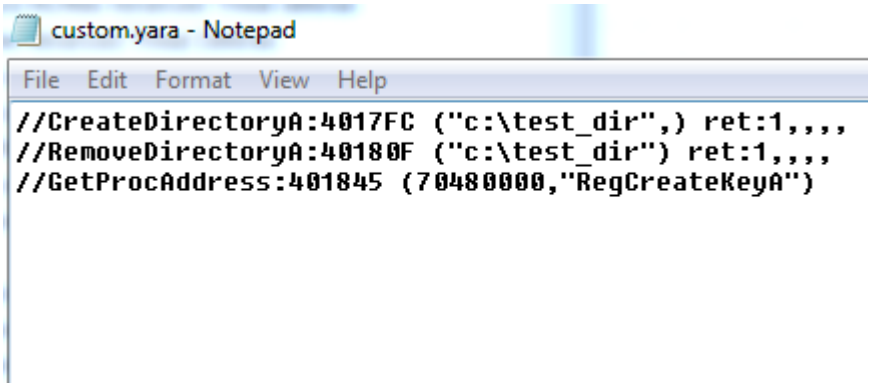



**Figure 6-8 Comments for the custom YARA rules file**

3 Write the first rule and provide it a name.

4 Enter the metadata for the rule.

Metadata is mandatory for standard rules and optional for helper rules. Regarding custom YARA rules, metadata can contain *classification*, *description*, and *severity*. Use a [metadata field name] = [string/value] format to define all these three metadata fields. These fields are case-insensitive.

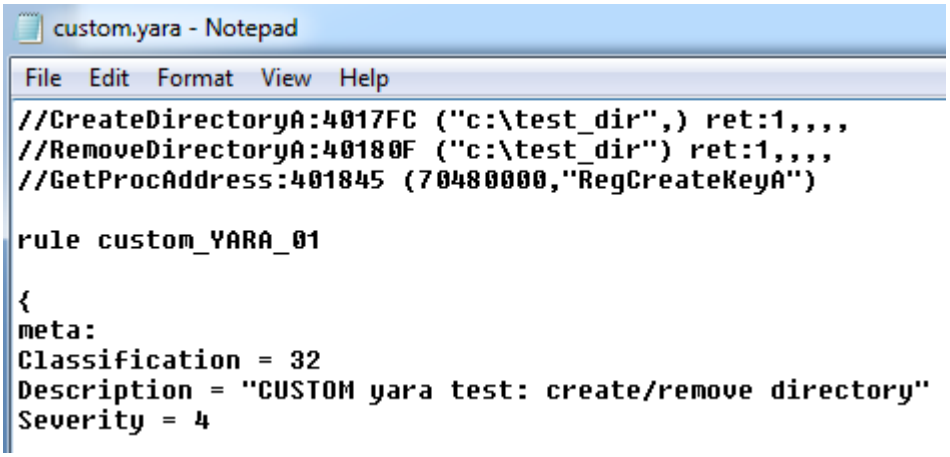



**Figure 6-9 Metadata for a custom YARA rule**

**a** Optionally, enter the classification value for the YARA rule. Classification is the malware classification category to which a behavioral rule belongs. Use the following information to calculate the classification value.

| Classification | Value |
|---|---|
| Persistence, Installation Boot Survival | 1 |
| Hiding, Camouflage, Stealthiness, Detection and Removal Protection | 2 |
| Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection | 4 |
| Spreading | 8 |
| Exploiting, Shellcode | 16 |
| Networking | 32 |
| Data spying, Sniffing, Keylogging, Ebanking Fraud | 64 |

For example, if a YARA rule describes a malware that attempted to do spreading (value 8), installation boot survival (value 1), and networking (value 32) then total classification result is 8+1+32 = 41.

**b** Enter the description for the rule, which is displayed in the analysis reports.

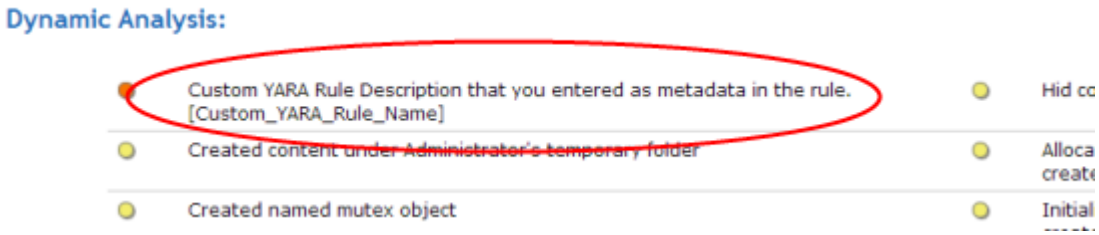



**Figure 6-10 Custom YARA rule name and description in the reports**

**c** Enter a severity value for the behavior described by the YARA rule.

Severity value must be an integer from 1–5, with 5 indicating most maliciousness behavior. Severity values are irrelevant for helper rules.

5 From the **Analysis Results** page, open the user API log report of the sample, which you plan to use as a reference to create the YARA rules.

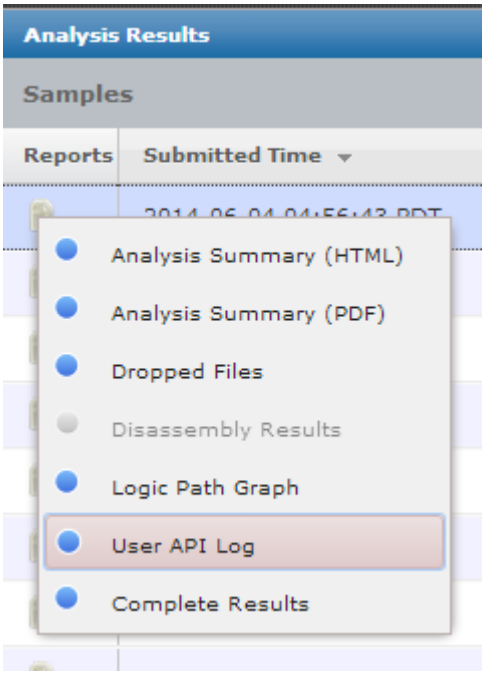



**Figure 6-11 User API log as a reference for custom YARA rules**

6 Enter the strings and conditions according to YARA syntax.

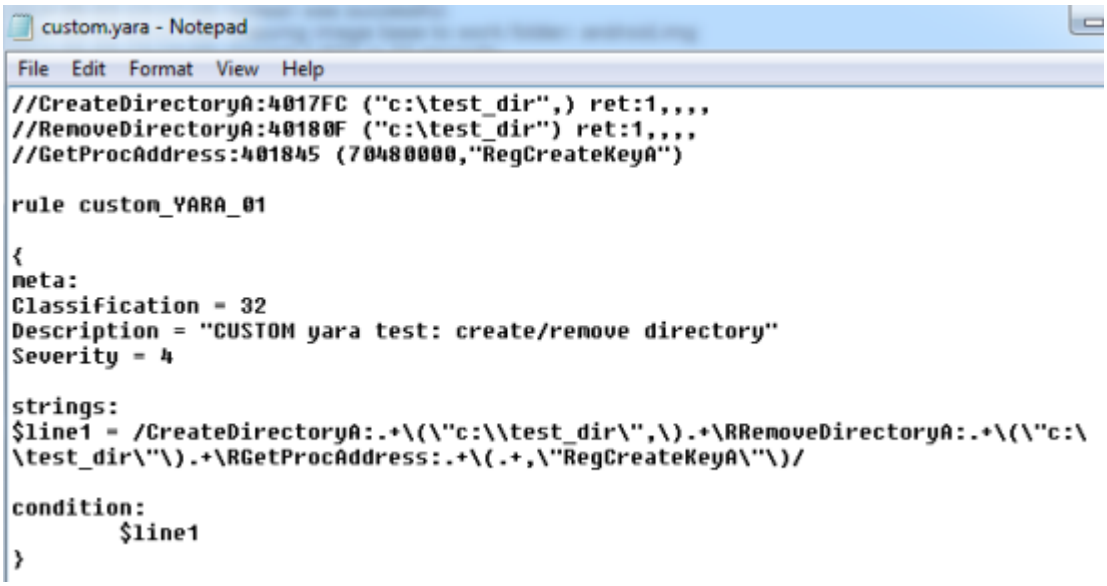



**Figure 6-12 A custom YARA rule**

7 Add more rules according to your requirement in the same custom YARA text file and save the file when complete.

The next step is to import this file into McAfee Advanced Threat Defense.

# Import the custom YARA rules file

**Before you begin**

You have defined your YARA rules in a text file as described in Create the custom YARA rules file on page 242.

After you create your YARA rules in a text file, you import this file into McAfee Advanced Threat Defense using the McAfee Advanced Threat Defense web application. After you import the custom YARA files and if you have enabled custom YARA rules, McAfee Advanced Threat Defense includes these YARA rules in its malware-detection mechanism.

## Task

1 Select **Manage** | **Custom YARA Rules**.

2 Select **Enable YARA Rules** checkbox.

Select this checkbox if you import a custom YARA text file. If necessary, you can later disable custom YARA rules.

3 Click **Browse** and locate the custom YARA text file that you created.

4 Click **Submit** to import the file.

If the file is imported successfully, a message is displayed.

If there are syntax errors in the YARA rules, the rules are not imported. An error message is displayed and you can review the system log for the details of the error. Suppose that an ending backslash is missing in a regular-expression string of a rule. When you import the custom YARA file containing such a rule, an error message is displayed.

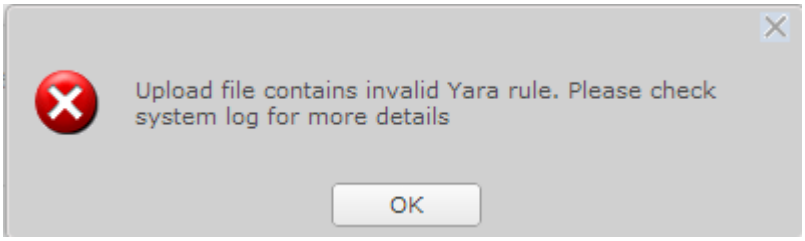



**Figure 6-13 Message indicating a syntax error**

Select **Manage** | **System Log** to open the system log, where the errors are detailed.

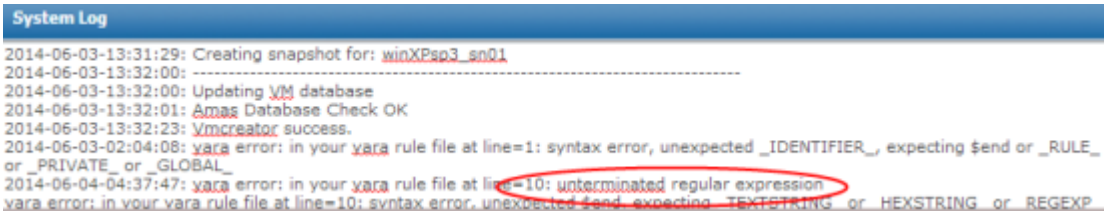

System Log
2014-06-03-13:31:29: Creating snapshot for: winXPsp3_sn01
2014-06-03-13:32:00: ----------
2014-06-03-13:32:00: Updating VM database
2014-06-03-13:32:01: Amas Database Check OK
2014-06-03-13:32:23: Vmcreator success.
2014-06-03-02:04:08: yara error: in your yara rule file at line=1: syntax error, unexpected _IDENTIFIER_, expecting $end or _RULE_ or _PRIVATE_ or _GLOBAL_
2014-06-04-04:37:47: yara error: in your yara rule file at line=10: unterminated regular expression
yara error: in your yara rule file at line=10: syntax error, unexpected $end, expecting _TEXTSTRING_ or _HEXSTRING_ or _REGEXP_

**Figure 6-14 Details of the error**

# Enable or disable custom YARA rules

**Before you begin**

You have imported the custom YARA text file into McAfee Advanced Threat Defense.

After you import the custom YARA rules, you can disable the custom YARA rules when not required. For example, you might want to disable them for reasons such as troubleshooting. However, when you disable custom YARA rules, it applies to all samples analyzed by that McAfee Advanced Threat Defense. Later, you can enable custom YARA rules as well.

### Task

1 Select **Manage** | **Custom YARA Rules.**

2 Deselect or select **Enable YARA Rules** checkbox to disable or enable custom YARA rules.

If you want to enable the YARA rules that are currently present in the McAfee Advanced Threat Defense database, select **Enable YARA Rules** checkbox and click **Submit.** That is, you need not import the custom YARA rules text file again.

## Modify custom YARA rules

**Before you begin**

You have imported the custom YARA text file into McAfee Advanced Threat Defense.

After you import the custom YARA rules, you might want to add some more rules or modify some of the existing rules. For example, you might want to change the severity value for a rule.

### Task

1 Select **Manage** | **Custom YARA Rules.**

2 Click **Download YARA Rule File** to download the `custom.yara` file from the McAfee Advanced Threat Defense database onto your client.

The timestamp of when the `custom.yara` file was last imported into McAfee Advanced Threat Defense is provided for your reference.

3 Open the `custom.yara` file that you downloaded in a text editor and make the required changes such as adding new rules, deleting an existing rule, or modifying an existing rule. When complete, save the file.

You can rename this file according to your requirement.

4 Import the modified custom YARA rules file into McAfee Advanced Threat Defense.

See Import the custom YARA rules file on page 245.

# 7 Analyzing malware

After you have configured McAfee Advanced Threat Defense, you can upload files and Uniform Resource Locators (URLs) for analysis. You can monitor the status of malware analysis using McAfee Advanced Threat Defense web application and then view the results.

**Contents**


- *Analyze files*
- *Analyze URLs*
- *Monitor the status of malware analysis*
- *View the analysis results*
- *Working with the McAfee Advanced Threat Defense Dashboard*


## Analyze files

- The following are the methods you can follow to submit files:
  - Manually upload the file using the McAfee Advanced Threat Defense web application.
  - Post the file on the FTP server hosted on the McAfee Advanced Threat Defense Appliance.
  - Use the restful APIs of McAfee Advanced Threat Defense web application to upload the file. See the *McAfee Advanced Threat Defense RESTful APIs Reference Guide.*
  - Integrate McAfee Advanced Threat Defense with Network Security Platform and McAfee Web Gateway. Then, these applications automatically submit samples to McAfee Advanced Threat Defense. See the corresponding documentation.
- The maximum file size supported is 128 MB if you use the McAfee Advanced Threat Defense web application, its restful APIs, or McAfee Web Gateway. In case of compressed files and APK files, the maximum size supported is 20 MB.
- If you use Network Security Platform, the maximum file size supported is 25 MB.
- With respect to the file name of samples, McAfee Advanced Threat Defense supports Unicode. So, the file names can contain non-English characters and some special characters except \'"` <>|; () []*?#$&:
- The file name can be up to 200 bytes in length.

**Table 7-1 Supported file types**

| File Types | Static Analysis | Dynamic Analysis |
|---|---|---|
| 32 - bit Portable Executables (PE files) | (.exe, .dll, .scr, .ocx, .sys, .com, .drv, .cpl) | (.exe, .dll, .scr, .ocx, .sys, .com, .drv, .cpl) |
| Microsoft Office Suite Documents | (.doc, .docx, .xls, .xlsx .ppt, .pptx, .rtf) | (.doc, .docx, .xls, .xlsx, .ppt, .pptx, .rtf) |
| Adobe | PDF Files, Adobe Flash files (SWF) | PDF Files, Adobe Flash files (SWF) |
| Compressed Files (The maximum file size supported is 20 MB) | (.zip, .rar) | (.zip) |
| Android Application Package | (.apk) | (.apk) |
| Java | Java Archives (JAR), CLASS | Java Archives (JAR), CLASS |
| Image files | (JPEG, PNG, GIF) | Not supported |

# Upload files for analysis using McAfee Advanced Threat Defense web application

**Before you begin**

The required analyzer profile is available.

When you use the McAfee Advanced Threat Defense web application to submit a file for analysis, you must select an analyzer profile. This analyzer profile overrides the default analyzer profile associated with your user account.

## Task

1 Select **Analysis** | **Manual Upload.**

2 In the **Manual Upload** page, specify the details as per your requirement.

**Table 7-2 Option definitions**

| Option | Definition |
|---|---|
| **File** | Either drag and drop the malware file from Windows Explorer or click **Browse** and select the file. If you want to submit multiple files, upload them in a .zip file.<br>• If you are uploading a password-protected .zip file, make sure you have provided the password in the analyzer profile that you want to use for analysis.<br>• If dynamic analysis is required, the files in the .zip file are executed on different instances of the analyzer VM. If enough analyzer VMs are not available, some of the files are in pipeline until analyzer VMs are available.<br>• Because the files in the .zip file are analyzed separately, separate reports are created for each file.<br>• With respect to the file name of samples, McAfee Advanced Threat Defense supports Unicode. So, the file names can contain non-English characters and some special characters except \'"` <>\|; ()[]*?#$&:<br>• The file name can be up to 200 bytes in length. |
| **Analyzer Profile** | Select the required analyzer profile for the sample. |
| **Advanced** | Click to specify additional parameters for analyzing the sample.<br>The **Advanced** options are available only when you manually submit the file using McAfee Advanced Threat Defense web application.<br>• **Region**: In some cases, the behavior of a file might vary based on the geographical location of the target system. For example, malware from a rogue nation might not cause any harm to computers in its own country or that of its friends. Select the country if you want to analyze the malware in relation to location.<br>You cannot modify the list of countries. This list might be updated when you upgrade McAfee Advanced Threat Defense software.<br>• **User Interactive Mode**: Upon execution, some malware require user input. This is typically done to check if the malware is being analyzed in a sandbox. In the absence of user input, the malware might take an alternative execution path or even might suspend further execution.<br>If you select this option, you can access the actual analyzer VM on which the malware is executed and provide the required input. See Upload URLs for analysis in user-interactive mode on page 249.<br>After you made the required selections, click **OK**. |
| **Submit** | Click to upload the file to McAfee Advanced Threat Defense for analysis. |

### Tasks

- *Upload URLs for analysis in user-interactive mode* on page 249

## Upload URLs for analysis in user-interactive mode

**Before you begin**

The required analyzer profile is available with sandbox and malware Internet access options selected.

To completely execute some malware, user intervention might be required. For example, a default setting in the analyzer VM might pause the execution unless the setting is manually overridden. Some files might display dialog boxes, where you are required to make a selection or a confirmation. Malware demonstrates such behavior to determine if they are being executed in a sandbox. The

behavior of the malware might vary based on your intervention. When you submit files in user-interactive mode, the analyzer VM is opened in a pop-up window on your client computer and you can provide your input when prompted.

You can upload files to be executed in the user-interactive mode. This option is available only when you manually upload a file using the McAfee Advanced Threat Defense web application. For files submitted by other methods, such as FTP upload and files submitted by Network Security Platform, requests for user-intervention by the malware are not honored. However, the screen shots of all such requirements are available in the **Screenshots** section of the **Analysis Summary** report. Then you can manually resubmit such files in the user-interactive mode to know the actual behavior of the file.

Because the analyzer VM is opened in a pop-up, make sure the pop-up blocker is disabled in your browser.

## Task

1 Select **Analysis** | **Manual Upload.**

2 In the **File** field, click **Browse** and select the file you want to submit for analysis or drag and drop the file into the specified box.

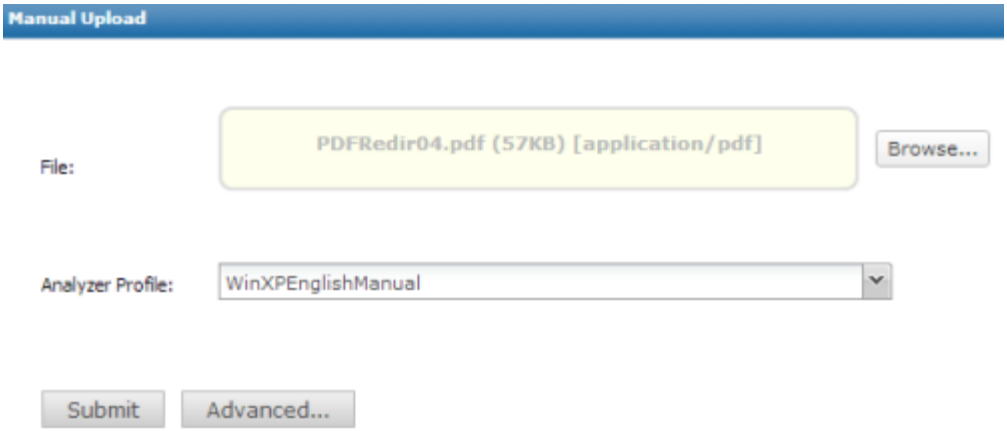



**Figure 7-1 Submit the file**

3 In the **Analyzer Profile** field, select the required analyzer profile from the drop-down list.

4 Click **Advanced...** and select **User Interactive Mode (XMode)**.

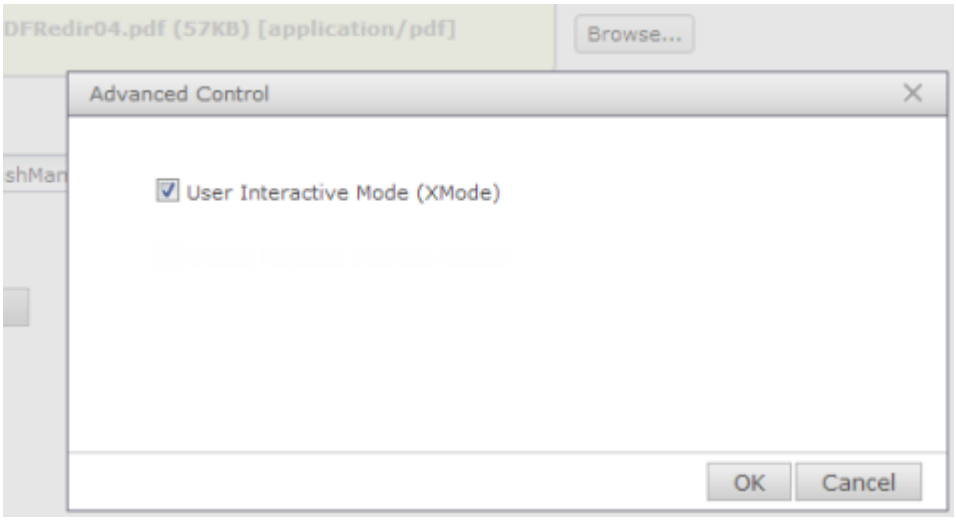



**Figure 7-2 Select User Interactive Mode (XMode)**

5 Click **OK** and then **Submit**.

The sample is uploaded to McAfee Advanced Threat Defense and a success message with the details are displayed.

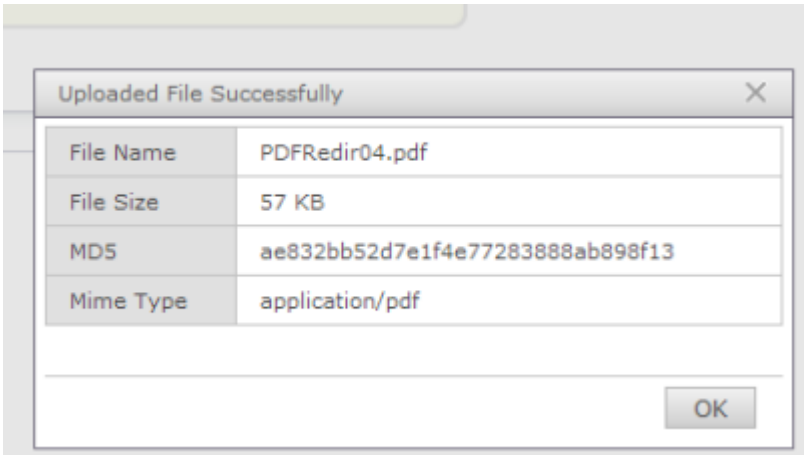



**Figure 7-3 File upload success message**

6 Click **OK** in the **Uploaded File Successfully** dialog.

7 You must go to the **Analysis Status** page to interact with the sample. So, click **OK** in the **User Interactive Mode** message box and select **Analysis** | **Analysis Status.**

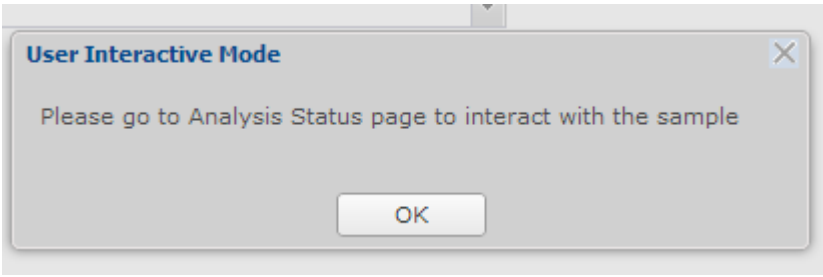



**Figure 7-4 User Interactive Mode message**

In the **Analysis Status** page, the **X-Mode** button is displayed in the **Status** column for the corresponding record.

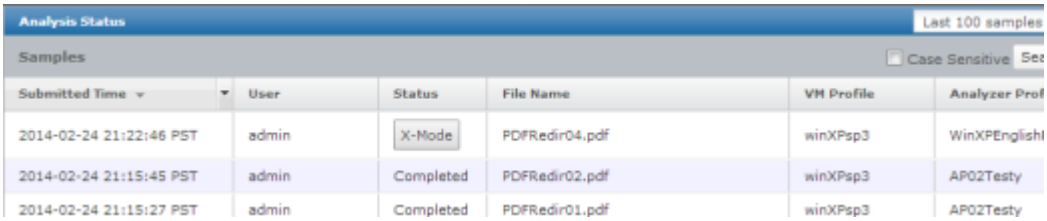



**Figure 7-5 X-Mode in the Analysis Status page**

8 Click **X-Mode** for the corresponding record in the **Analysis Status** page.

A pop-up window opens in your machine. Security warnings might be displayed based on your browser and Java settings. After you confirm the security warnings, the analyzer VM is displayed in

the pop-up window and the dialog boxes opened by the sample are displayed. You can use your mouse and keyboard to provide your input.

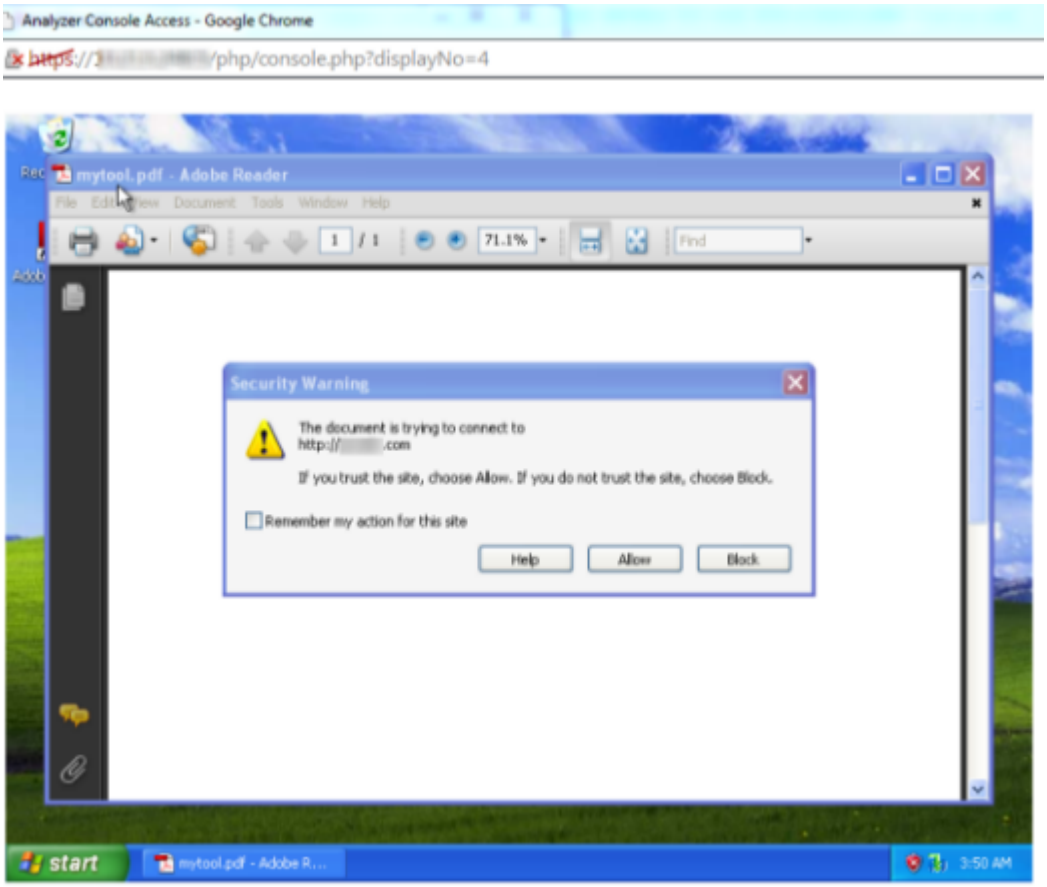



**Figure 7-6 Analyzer VM accessible in a pop-up window**

Execution of the file begins as soon as you submit the file. It does not wait until you open the analyzer VM. Some messages might timeout in the background. To view the complete execution, you must click **X-Mode** in the **Analysis Status** page without delay.

After the file completes execution, the analyzer VM logs off automatically and you can close the pop-up.

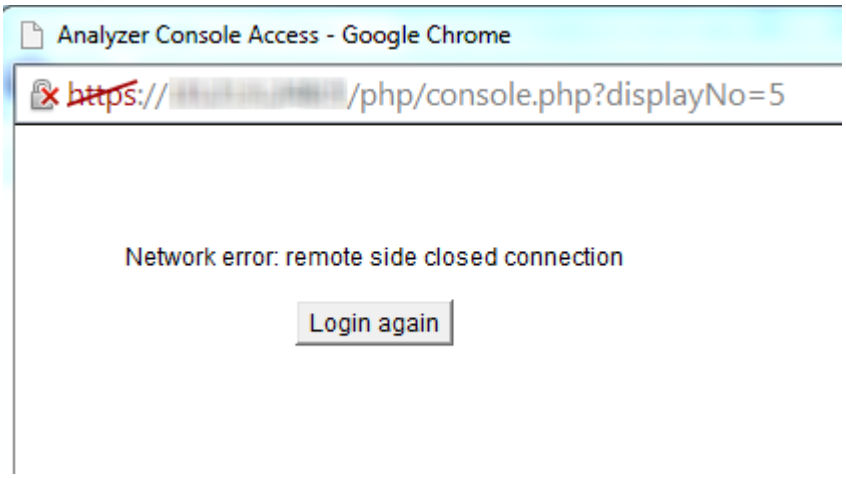



**Figure 7-7 Analyzer VM logs off**

## Upload files for analysis using SFTP

**Before you begin**

- Your user name has **FTP Access** privilege. This is required to access the FTP server hosted on McAfee Advanced Threat Defense.
- You have created the required analyzer profile that you want to use.
- You have installed an FTP client on your machine.

Using SFTP, you can upload the supported file types to the FTP server on McAfee Advanced Threat Defense.

By default, FTP is not a supported protocol for uploading samples. To use FTP to upload files, you must enable it using the `set ftp` CLI command. See set ftp on page 314.

**Task**

1. Open your FTP client and connect to McAfee Advanced Threat Defense using the following information.
   - Host — Enter the IP address of McAfee Advanced Threat Defense.
   - User name — Enter your McAfee Advanced Threat Defense user name.
   - Password — Enter your McAfee Advanced Threat Defense password.
   - Port — Enter 22, which is the standard port for SFTP. For FTP, enter 21.
2. Upload the files from the local site to the remote site, which is on McAfee Advanced Threat Defense.
3. In the McAfee Advanced Threat Defense web application, select **Analysis** | **Analysis Status** to monitor the status of the uploaded files.

# Analyze URLs

Similar to how you submit a file for analysis, you can submit URL to Advanced Threat Defense for analysis in this release. Advanced Threat Defense downloads the file stored at the URL in an analyzer VM determined by the user profile and reports the file analysis results. Advanced Threat Defense uses only the local blacklist and dynamic analysis for the downloaded file. In addition, the McAfee GTI reputation of the URL is reported. The behavior of the browser when opening the URL is also analyzed for malicious activity.

Follow these methods to submit URLs:

- Manually upload the URL using the Advanced Threat Defense web application.
- Use the restful APIs of Advanced Threat Defense web application to upload URLs. See the *Advanced Threat DefenseRESTful APIs Reference Guide.*

Malicious websites typically contain multiple types of malware. When a victim visits the website, the malware that suits the vulnerabilities present in the endpoint is downloaded. You can create multiple analyzer VMs, each with different operating systems, browsers, applications, browser plug-ins that are relevant to your network. Also, if the browsers and operating systems are unpatched, it might enable you to analyze the actual behavior of web sites.

The advantage of using Advanced Threat Defense is that, you can get a detailed report of previously unknown malicious domains, websites, and IP addresses as well as the current behavior of known ones. You can also get a detailed analysis report for even benign sites that are recently compromised.

Advanced Threat Defense does not analyze URLs contained within files submitted for analysis. For example, when a Network Security Sensor submits a Microsoft Word file, Advanced Threat Defense analyses the file for malware but does not analyze any URLs in the file.

## How Advanced Threat Defense analyzes URLs?

To analyze URLs, select an analyzer profile that has both sandbox and Internet access enabled. Following is the process flow when you submit a URL for analysis to Advanced Threat Defense:

1 Advanced Threat Defense uses a proprietary procedure to calculate the MD5 hash value of the URL. Then, it checks this MD5 against its local blacklist.

The local whitelist is not applicable for URLs.

2 It is assumed that the file that the URL refers to is of a supported file type. Then Advanced Threat Defense dynamically analyzes the file using the corresponding analyzer VM. It is assumed that the MD5 of the URL is not present in the blacklist or **Run All Selected** option is selected in the corresponding analyzer profile.

GTI File Reputation, Anti-Malware, and Gateway Anti-Malware analyze options are not relevant for URLs.

3 Dynamic analysis and reporting for URLs is similar to that of files. It records all activities in the analyzer VM including registry operations, process operations, file operations, runtime DLLs, and network operations. If the webpage downloads any dropper files, Advanced Threat Defense dynamically analyzes these files as well and includes the results in the same report under embedded/dropped content section.

4 If a dropped file connects to other URLs, all these URLs are checked with TrustedSource for URL reputation and categorization.

Only HTTP, HTTPS, and FTP protocols are supported for URL analysis.

## Upload URLs for analysis using Advanced Threat Defense web application

**Before you begin**

The required analyzer profile is available with sandbox and malware Internet access options selected.

When you use the Advanced Threat Defense web application to submit a URL for analysis, select an analyzer profile. This analyzer profile overrides the default analyzer profile associated with your user account.

## Task

1 Select **Analysis** | **Manual Upload.**

2 In the **Manual Upload** page, specify the details according to your requirement.

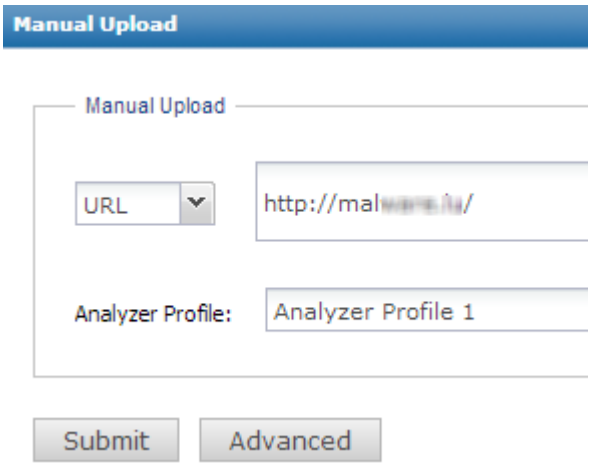



**Figure 7-8 Submit a URL for malware analysis**

**Table 7-3 Option definitions**

| Option | Definition |
|---|---|
| **URL** | Select **URL** from the drop-down list and enter the URL in the adjacent text box.<br>Only HTTP, HTTPS, and FTP are supported. So, specify the protocol identifier in the URL.<br>Preferably enter the entire URL. When Advanced Threat Defense dynamically analyzes the URL, the browser might add any missing items. For example, if you enter `http://google.com`, the browser in the analyzer VM might correct it to `http://www.google.com` |
| **Analyzer Profile** | Select the required analyzer profile for the sample.<br>Only those analyzer profiles that have sandbox and malware Internet access are listed. |

**Table 7-3 Option definitions** *(continued)*

| Option | Definition |
|---|---|
| **Advanced** | Click to specify user interactive mode for analyzing the URL.<br><br>The **Advanced** option is available only when you manually submit the file using McAfee Advanced Threat Defense web application.<br><br>Upon execution, some malware require user input. This is typically done to check if the malware is being analyzed in a sandbox. In the absence of user input, the malware might take an alternative execution path or even might suspend further execution.<br><br>If you select this option, you can access the actual analyzer VM on which the malware is executed and provide the required input. This is similar to executing files in user-interactive mode. See Upload URLs for analysis in user-interactive mode on page 249. |
| **Submit** | Click to upload the URL to McAfee Advanced Threat Defense for analysis.<br>A message box is displayed after the URL is uploaded successfully.<br>• File Name — The URL that you submitted.<br>• File Size — Size of the sample.<br>• MD5 — The MD5 hash value as computed by Advanced Threat Defense.<br>• Mime Type. |

# Monitor the status of malware analysis

After you submit a file for analysis, you can monitor the status from the **Analysis Status** page.

## Task

1 Select **Analysis** | **Analysis Status**.

The **Analysis Status** page lists the status for the submitted files.

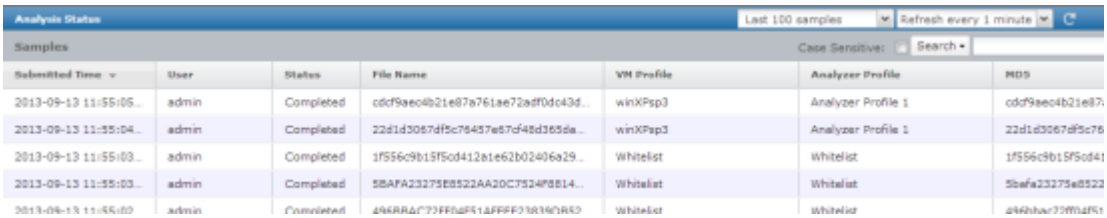



**Figure 7-9 Status of files submitted for analysis**

If you do not have admin permissions, only those files that you submitted are listed. A user with admin permissions can view the samples provided by any user.

2 Specify the criteria for viewing and refreshing the status of files being analyzed.

a Set the criteria to display records in the **Analysis Status** page.

You can specify this criteria based on time or number. For example, you can select to view the status for files submitted in the last 5 minutes or for the last 100 samples.

b Set the frequency at which the **Analysis Status** page must refresh itself.

The default refresh interval is 1 minute.

c To refresh the **Analysis Status** page now, click .

3

4 Filter the displayed records to locate the required ones.

**Table 7-5 Filtering options**

| Option | Definition |
|---|---|
| **Search** | Specify the parameter that you want to use to filter the records. Click **Search** and select one or more of the following parameters:<br>• **File Name:** Select if you want to filter based on the starting characters of the file name. For example, if you select this option and enter *cal* as the search string then the status for files names that start with *cal* are listed.<br>• **MD5:** Select if you want to filter based on the starting characters of the MD5 hash value.<br>• **Status:** Select if you want to filter based on the status - Waiting, Analyzing, or Completed.<br>Enter the search string in the adjacent text box. |
| **Case Sensitive** | Select if you want to make the search case sensitive. |

Suppose that you have selected **File Name** and **Status** as the criteria, selected **Case Sensitive**, and specified *Com*. All the records in the completed state and file names starting with the characters *Com* are listed.

**Table 7-6 Column definitions**

| Column | Definition |
|---|---|
| **Submitted Time** | The time stamp when the file was submitted for analysis. |
| **User** | The log on name of the user who submitted the file for analysis. |
| **Status** | The current status of analysis.<br>• **Waiting —** Typically, this indicates that McAfee Advanced Threat Defense is waiting for an analyzer VM to dynamically analyze the file.<br>• **Analyzing —** Indicates that the analysis is still in progress.<br>• **Completed —** Indicates that the analysis is complete for the file. Double-click the record to see the complete report. |
| **File Name** | The name of the file that you submitted for analysis. |
| **VM Profile** | The VM profile used for dynamic analysis. If the file was analyzed only by a static method, that is displayed. |
| **Analyzer Profile** | The analyzer profile that was referred to for the analysis. If the file was analyzed only by a static method, that is displayed. |
| **MD5** | The MD5 hash value of the file as calculated by McAfee Advanced Threat Defense. |
| **File Type** | The file type of the sample, such as binary. |

5 Hide the columns that you do not require.

a Move the mouse over the right corner of a column heading and click the drop-down arrow.

b Select **Columns**.

c Select only the required column names from the list.

You can click a column heading and drag it to the required position.

6 To sort the records based on a particular column name, click the column heading.

You can sort the records in the ascending or descending order. Alternatively, move the mouse over the right corner of a column heading and click the drop-down arrow. Then select **Sort Ascending** or **Sort Descending**.

# View the analysis results

After you submit a file for analysis, you can view the results in the **Analysis Results** page.

Older reports are deleted when the data disk of McAfee Advanced Threat Defense is 75 percent full. You can view the current data disk space available in the **System Health** monitor of the **Dashboard**. If you configure the options under **FTP Result Output** in the **User Management** page, then McAfee Advanced Threat Defense saves the results locally as well as sends them to the configured FTP server for your long-term use.

## Task

1 Select **Analysis** | **Analysis Results**.

The **Analysis Results** page lists the status for the completed files.

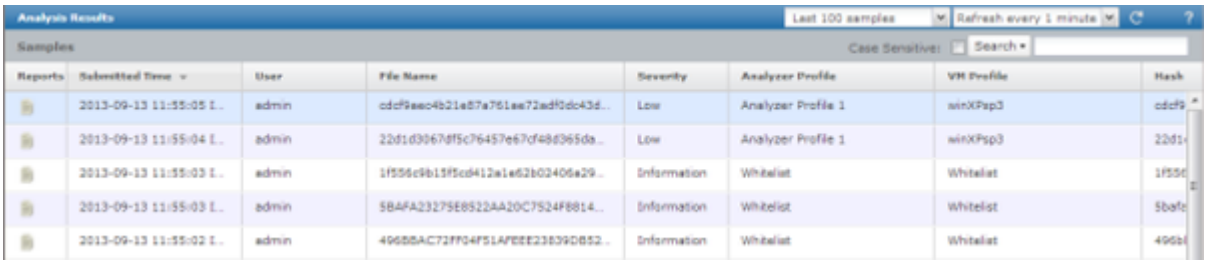



**Figure 7-10 Status of files submitted for analysis**

If you do not have admin permissions, only those files that you submitted are listed. A user with admin permissions can view the samples submitted by all users.

2 Specify the criteria for viewing and refreshing the records in the **Analysis Results** page.

a Set the criteria to display records in the **Analysis Results** page.

You can specify this criteria based on time or number. For example, you can select to view the files for which the analysis was completed in the last 5 minutes or for the last 100 completed files.

b Set the frequency at which the **Analysis Results** page must refresh itself.

The default refresh interval is 1 minute.

c To refresh the **Analysis Results** page now, click .

**Table 7-7 Column definitions**

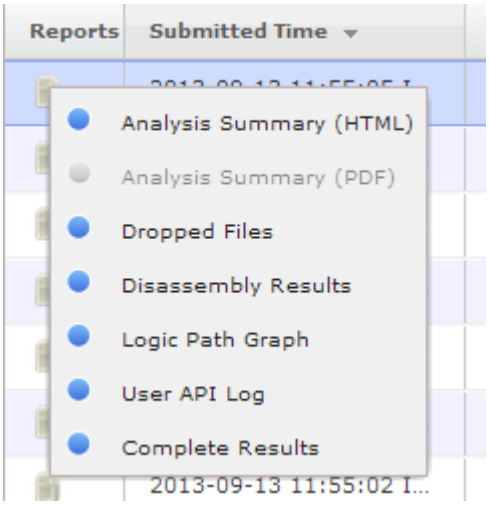
| Column | Definition |
|---|---|
| **Reports** | Click to display the types of reports available for the sample.<br>  <br>Click any of the enabled reports to view the corresponding details. A specific report is enabled only if it is relevant to the analyzed file and also selected in the corresponding analyzer profile.<br>• **Analysis Summary (HTML)** — This is the comprehensive report that is available for all file types. This report is also displayed when you double-click a record.<br>• **Analysis Summary (PDF)** — Select this to view the report in PDF.<br>• **Dropped Files** — Select this report to view the files that the analyzed sample created during dynamic analysis.<br>• **Disassembly Results** — Select this to view the assembly language code reverse-engineered from the file. This report is relevant only for sample types such as .exe and .dll.<br>• **Logic Path Graph** — Select this to view a graphical representation of which subroutines were executed during the dynamic analysis and which were not.<br>• **Dynamic Execution Logs** — Select this to view the Windows user-level DLL API calls made directly by the sample during dynamic analysis.<br>• **Complete Results** — Click to download the .zip file containing all the report types to your local machine. |
| **Submitted Time** | The time stamp when the file was submitted for analysis. |
| **User** | The log on name of the user who submitted the file for analysis. |

**Table 7-7 Column definitions** *(continued)*

| Column | Definition |
|---|---|
| **Severity** | Indicates the severity level of the analyzed sample.<br>• Information — Indicates that this is a clean file. White-listed files have this severity level. Corresponds to a severity score of zero.<br>• Very low — Corresponds to a severity score of 1.<br>• Low — Corresponds to a severity score of 2.<br>• Medium — Corresponds to a severity score of 3.<br>• High — Corresponds to a severity score of 4.<br>• Very high — Corresponds to a severity score of 5. |
| **File Name** | The name of the file that you submitted for analysis. |
| **Analyzer Profile** | The analyzer profile that was referred to for the analysis. |
| **VM Profile** | The VM profile used for the dynamic analysis. If only static was used, that is displayed. |
| **Hash** | The MD5 hash value of the file as calculated by McAfee Advanced Threat Defense. |
| **File Size** | The size of the analyzed file in KB. |

3 Choose to hide the columns that you do not require.

a Move the mouse over the right corner of a column heading and click the drop-down arrow.

b Select **Columns**.

c Select only the required column names from the list.

You can click a column heading and drag it to the required position.

4 To sort the records based on a particular column name, click the column heading.

You can sort the records in the ascending or descending order. Alternatively, move the mouse over the right corner of a column heading and click the drop-down arrow. Then select **Sort Ascending** or **Sort Descending**.

## View the Analysis Summary report

The Analysis Summary report is an executive brief detailing key behaviors of the sample file. This report is available in HTML, text, PDF, XML, JSON, Open Indicators of Compromise (OpenIOC), and Structured Threat Information eXpression (STIX) formats.

The HTML, text, and PDF formats are mainly for you to review the analysis report. You can access the HTML and PDF formats from the McAfee Advanced Threat Defense web application. The HTML and text formats are also available in the reports .zip file for the sample, which you can download to your client computer.

The XML and JSON formats provide well-known malware behavior tags for high-level programming script to extract key information. Network Security Platform and McAfee Web Gateway use the JSON formats to display the report details in their user interfaces.

If the severity level of the sample is 3 and above, then the Analysis Summary report is available in OpenIOC (.ioc) and STIX (.stix.xml) formats. OpenIOC and STIX formats are universally recognized formats for sharing threat information. These formats enable you to effectively share the Analysis Summary reports with other security applications for a better understanding, detection, and

containment of malware. For example, you can manually submit the OpenIOC and STIX reports to an application, which can query hosts for the indicators in the report. This way you can detect the infected hosts, and then take the required remedial actions to contain and remove the malware.

For generic information on OpenIOC, see http://www.openioc.org/. Regarding STIX, you can see https://stix.mitre.org/. The Analysis Summary report in the OpenIOC and STIX formats are available in the Complete Results zip file for the sample.

## Task

1 To access the Analysis Summary report in the McAfee Advanced Threat Defense web application, do the following:

   a Select **Analysis** | **Analysis Results**.

   b To view the HTML format of the report, click and then select **Analysis Summary (HTML)**.

   Alternatively, you can double-click the required record.

   c To view the PDF of the report, click and then select **Analysis Summary (PDF)**.

2 To access the Analysis Summary report from the reports .zip file, do the following:

   a Select **Analysis** | **Analysis Results**.

   b Click and select **Complete Results**.

   c Save the zipped reports on your local machine.

   The .zip file is named after the name of the sample file.

   d Extract the contents of the .zip file.

   The AnalysisLog folder contains the HTML, text, XML, and JSON formats of the Analysis Report. If the malware severity is 3 and above, then it contains OpenIOC and STIX formats as well. You can identify these files by the malware file name. The malware file name is appended to _summary.html, _summary.json, _summary.txt, _summary.xml, _summary.ioc, and _summary.stix.xml.

The various sections of the HTML format of the Analysis Summary report are outlined here.

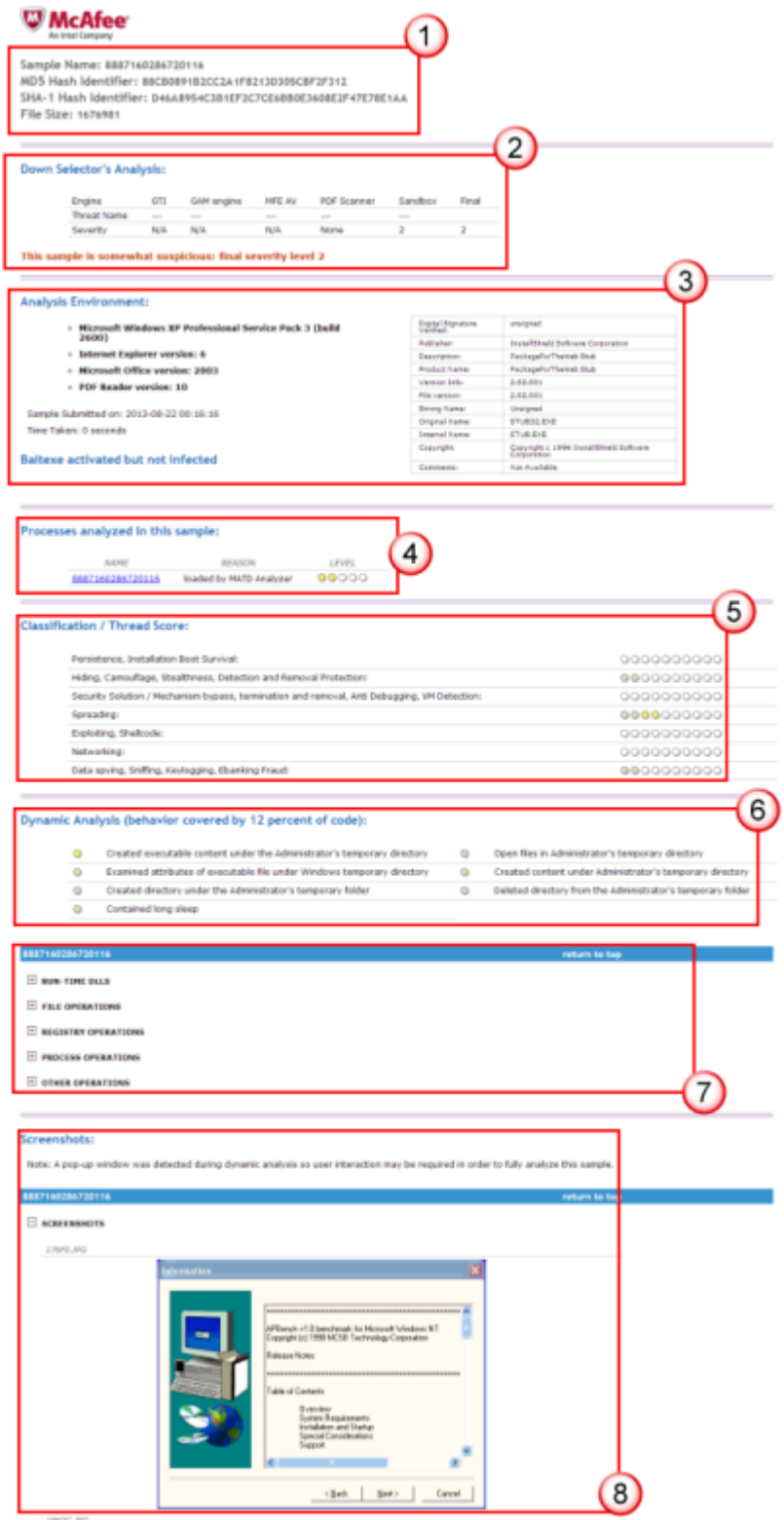



**Figure 7-11 Analysis Summary report**

**Table 7-8 Analysis Summary report sections**

| Item | Description |
|---|---|
| 1 | This section displays the details of the sample file. This includes the name, hash values, and the file size in bytes. |
| 2 | Analysis Results section on page 265. This section provides the results from the methods used for the file and the results from those methods. This section also displays the overall severity level for the file. |
| 3 | Analysis Environment section on page 265. This section includes the details of the analyzer VM, properties of the file, and so on. |
| 4 | Processes analyzed in this sample. This section lists all the files that were executed when dynamically analyzing the sample file. It also provides the reason how each file got to be executed along with their severity score.<br>The Reason column indicates which other file or process created or opened this file. If there is only one file in the sample, the reason displayed is *loaded by MATD Analyzer*. If the sample file is a .zip file containing multiple files or if a file opens other files, the reason for the first file is *created by <file name> & loaded by MATD Analyzer.* For the subsequent files, the Reason column indicates all the files/processes that created it and all the files/processes that opened it.<br>The Level column indicates the severity level based on dynamic analysis for each file.<br>• ○○○○○ — indicates a severity score of 0 and a threat level of informational. This is the severity for white-listed files.<br>• ○○○○○ — indicates a severity score of 1 and a threat level of very low.<br>• ●●○○○ — indicates a severity score of 2 and a threat level of low.<br>• ●●●○○ — indicates a severity score of 3 and a threat level of medium.<br>• ●●●●○ — indicates a severity score of 4 and a threat level of high.<br>• ●●●●● — indicates a severity score of 5 and a threat level of very high.<br>Click a file name to navigate to the section of the report that provides the details of the file behavior. That is, when you click a file name, you are navigated to the section indicated by 7 in the preceding figure. |
| 5 | Classification / threat score section on page 266. This section provides the individual scores for the various characteristics of a typical malware. |
| 6 | Dynamic analysis section. This section displays the percentage of the file code that was executed. For example, the file might have taken an alternative path during execution due to which some part of the code was not executed at all. This section also provides a brief executive behavior summary with the corresponding severity levels.<br>● indicates a very low severity behavior.<br>● indicates a low severity behavior.<br>● indicates a medium severity behavior.<br>● indicates a high severity behavior.<br>● indicates a very high severity behavior. |
| 7 | Operations details section. This section provides detailed information on all the operations performed by the sample file during dynamic analysis. These operations are grouped under corresponding groups. Expand each group for the specific operations. For example, expand **Files Operations** to view the files created, files deleted, files modified, files read, directories created or opened, directories removed, and so on. |

**Table 7-8 Analysis Summary report sections** *(continued)*

| Item | Description |
|---|---|
| 8 | GTI URL Reputation. This provides McAfee GTI reputation and severity for the URL. |
| 9 | Network activity. This section provides the details of every network operation during dynamic analysis of the sample. |
| 10 | Screen-shots section. This section displays all the pop-up windows during dynamic analysis. By viewing these screenshots, you can determine if user intervention is required during dynamic analysis to know the actual behavior of the file. If user intervention is required, you can submit the file manually in user-interactive mode. |

## Analysis Results section

This is a section in the Analysis Summary report. In this section, you can view which methods reported that a sample file contains a malware.

**Table 7-9 Down Selector's Analysis**

| Label | Description |
|---|---|
| **Engine** | These are the possible methods that McAfee Advanced Threat Defense uses to analyze a file.<br>• GTI File Reputation: Indicates McAfee GTI that is on the cloud.<br>• Gateway Anti_Malware: Indicates McAfee Gateway Anti-Malware engine.<br>• Anti-Malware: Indicates McAfee Anti-Malware Engine.<br>• Sandbox: Indicates that the file was executed in an analyzer VM. Refer to the Analysis Environment section within the report to know the details of that VM. |
| **Threat Name** | Indicates the name for known malware in McAfee GTI, McAfee Gateway Anti-Malware engine, and McAfee Anti-Malware Engine. |
| **Severity** | Indicates the severity score from various methods. The highest severity score by a particular method is used to assign the final severity level for the sample. |

## Analysis Environment section

This is a section in the Analysis Summary report. You can find the following details in this section:

- Details of the corresponding analyzer VM such as the operating system, browser and version, and the applications and their versions installed on the analyzer VM.

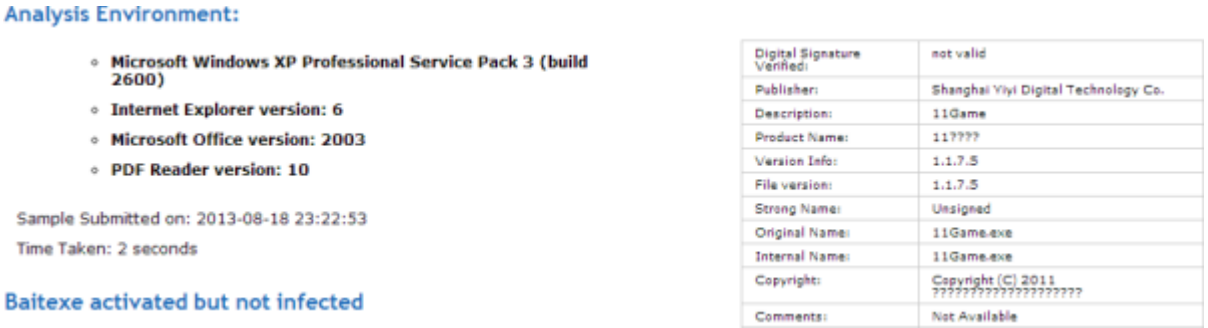

Analysis Environment:
Microsoft Windows XP Professional Service Pack 3 (build 2600)
Internet Explorer version: 6
Microsoft Office version: 2003
PDF Reader version: 10
Sample Submitted on: 2013-08-18 23:22:53
Time Taken: 2 seconds
Baitexe activated but not infected
Digital Signature Verified: not valid
Publisher: Shanghai Yiyi Digital Technology Co.
Description: 11Game
Product Name: 11????
Version Info: 1.1.7.5
File version: 1.1.7.5
Strong Name: Unsigned
Original Name: 11Game.exe
Internal Name: 11Game.exe
Copyright: Copyright (C) 2011 ??????????????????
Comments: Not Available

**Figure 7-12 Analysis Environment section**

- The time when the sample was submitted as per McAfee Advanced Threat Defense Appliance's clock.
- The time taken to analyze the file and generate the reports.

- On the right-hand side, a table provides the properties of the file. This includes information such as:
  - Signed or unsigned for the digital signature of the file.
  - Publisher's name if available.
  - Version details
  - Original name of the file so that you can search other sources such as the web.
- *Baitexe* process infected or not. At the end of each analysis McAfee Advanced Threat Defense creates an additional bait process called Baitexe. This Baitexe program calls two APIs (beep and sleep) only continuously. If this Baitexe process is infected by the previously executed sample, the behavior of Baitexe is different. In this case, a message *Baitexe activated and infected* is displayed. If the Baitexe process is not infected at all, the message *Baitexe activated but not infected* is displayed.

## Classification / threat score section

This is a section in the Analysis Summary report, which provides the severity scores for various characteristics of a typical malware.

**Table 7-10 Classification / threat score section**

| Label | Description |
|---|---|
| **Persistence, Installation Boot Survival** | Some malware have the capability to remain on the infected host. This is referred to as persistence. Installation boot survival refers to the capability of the malware to sustain even after a restart. |
| **Hiding, Camouflage, Stealthness, Detection and Removal Protection** | This refers to the capability of the malware to evade detection and removal. |
| **Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection** | This refers to the capability of the malware to bypass or mislead detecting methods and engines. Some malware has anti-disassembly code, which can confuse or delay malware analysis. Some malware attempt to determine if they are being executed in a sandbox. If true, they might take a different execution path. This score indicates the presence of such code in the malware. |
| **Spreading** | Indicates the capability of the malware to spread across the network. |
| **Exploiting, Shellcode** | Indicates the presence of shellcode that can exploit a running program. |
| **Networking** | Indicates the network-related behavior of the malware during dynamic analysis. For example, the malware might have triggered DNS queries or created sockets. If there is a severity score provided for this characteristic, correlate with the Network Operations details for the files in the sample. |
| **Data spying, Sniffing, Keylogging, Ebanking Fraud** | Indicates if the malware is capable of any such behaviors. |

## Operations details section

This section provides the details of every operation performed by a file during dynamic analysis. Separate sections are provided for every file that was executed as part of the sample.

- Run-time DLLs: Lists all the DLLs and their paths that were called by a file in runtime.
- File operations: Lists file operation activities like creation, open, query, modification, copy, move, deletion, and directory creation/deletion operations. This section also lists the file attributes and the MD5 hash value for the files.
- Registry operations: Provides the details of Windows registry operation activities like creation/open, deletion, modification, and query on registry sub-key and key entry.

- Process operations: Details the process operation activities such as new process creation, termination, new service creation, and code injection into other processes.
- Networking operations: Details networking operations such as DNS queries, TCP socket activities, and HTTP file download.
- Other operations: Provides details of operations not belonging to these categories. Examples are mutex signally objects, getting the system metric and configuration data of the analyzer VM.

## Dropped files report

You can download a .zip file containing all the files that the sample created or touched during dynamic analysis. You can download these files using one of the following methods.

- In the **Analysis Results** page (**Analysis** | **Analysis Results**), click and select **Dropped Files**. Download the dropfiles.zip file, which contains the files that the sample created in the sandbox. To use this option, you must have enabled the **Dropped Files** option in the corresponding analyzer profile.
- After you click , select **Complete Results**. Download the <sample_name>.zip file. This .zip file contains the same dropfiles.zip inside the AnalysisLog folder. The Complete Results contains the dropfiles.zip regardless of whether you have enabled **Dropped Files** option in the corresponding analyzer profile.

## Disassembly Results

The Disassembly Results report provides the disassembly output listing for Portable Executable (PE) files. This report is generated based on the sample file after the unpacking process has completed. It provides detail information about the malware file such as, the PE header information.

The Disassembly Results report includes the following information:

- Date and time of the creation of the sample file
- File PE and Optional Header information
- Different section headers information
- The Intel disassembly listing

You can view the Disassembly Results report in the McAfee Advanced Threat Defense web application or download it as a file to your client computer. The contents of the report are the same in both the methods.

- To view the Disassembly Results report in the McAfee Advanced Threat Defense web application, select **Analysis** | **Analysis Results**. In the **Analysis Results** page, click and select **Disassembly Results**. To use this option, you must have enabled the **Disassembly Results** option in the corresponding analyzer profile.
- To download the report as a file, click in the **Analysis Results** page and select **Complete Results**. Download the <sample_name>.zip file. This .zip file contains a file named as <file name>_detail.asm in the AnalysisLog folder. The Zip Report contains this .asm file regardless of whether you have enabled **Disassembly Results** option in the corresponding analyzer profile.

The Disassembly Results report provides the assembler instructions along with any static standard library call names like printf and Windows system DLL API call names embedded in the listing. If the global variables such as string text are referenced in the code, these string texts are also listed.

**Table 7-11 A section of a sample Disassembly Results report**

| Column 1 | Column 2 | Column 3 |
|---|---|---|
| :00401010 | e8 1f2c0000 | call 00403c34<br>;;call URLDownloadToFileA |

The virtual address of the instruction is shown in column 1, the binary instruction in column 2, and the assembly instruction with comments is in column 3. In the preceding example the `call 00403c34` instruction at memory location of `00401010` is making a functional call at `0x403c34` memory location, which is determined to be system DLL API function call determined to be `URLDownloadToFileA()`. The comment shown with the `;;` in this listing provides the library function name.

## Logic Path Graph

This report is a graphical representation of cross-reference of function calls discovered during dynamic analysis. This report enables you to view the subroutines in the analyzed file that were executed during the dynamic analysis as well as the ones that were potentially not executed. These non-executed functions could be a potential time-bomb waiting to trigger under the right conditions.

The Logic Path Graph report is available as a Graph Modeling Language (GML) file. This file is an ASCII plain text format, which contains a graphical representation of the logic execution path of the sample in the GML (Graph Modeling Language) format. You cannot directly view this file in the McAfee Advanced Threat Defense web application, but download it to your client computer. Then you must use a graphical layout editor, like yWorks yEd Graph Editor, that supports GML format. You can use such an editor to display the cross-reference of all functions using this file as an input.

You can download the Logic Path Graph file using one of the following methods.

- In the **Analysis Results** page (**Analysis** | **Analysis Results**), click and select **Logic Path Graph**. Then download the <file name>_logicpath.gml file. To use this option, you must have enabled the **Logic Path Graph** option in the corresponding analyzer profile.
- After you click , select **Complete Results**. Download the <sample_name>.zip file. This .zip file contains the same <file name>_logicpath.gml file in the AnalysisLog folder. The Zip Report contains the <file name>_logicpath.gml file regardless of whether you have enabled **Logic Path Graph** option in the corresponding analyzer profile.

This section uses yWorks yEd Graph Editor to explain how to use the Logic Path Graph GML file. In the yEd Graph Editor, you must first set the Routing Style. You need to do this only once, and this setting is saved for further use.

1 In the yEd Graph Editor, select **Layout** | **Hierarchical.**

2 In the **Incremental Hierarchic Layout** dialog, select the **Edges** tab and select **Polyline** from the **Routing Style** drop-down list.

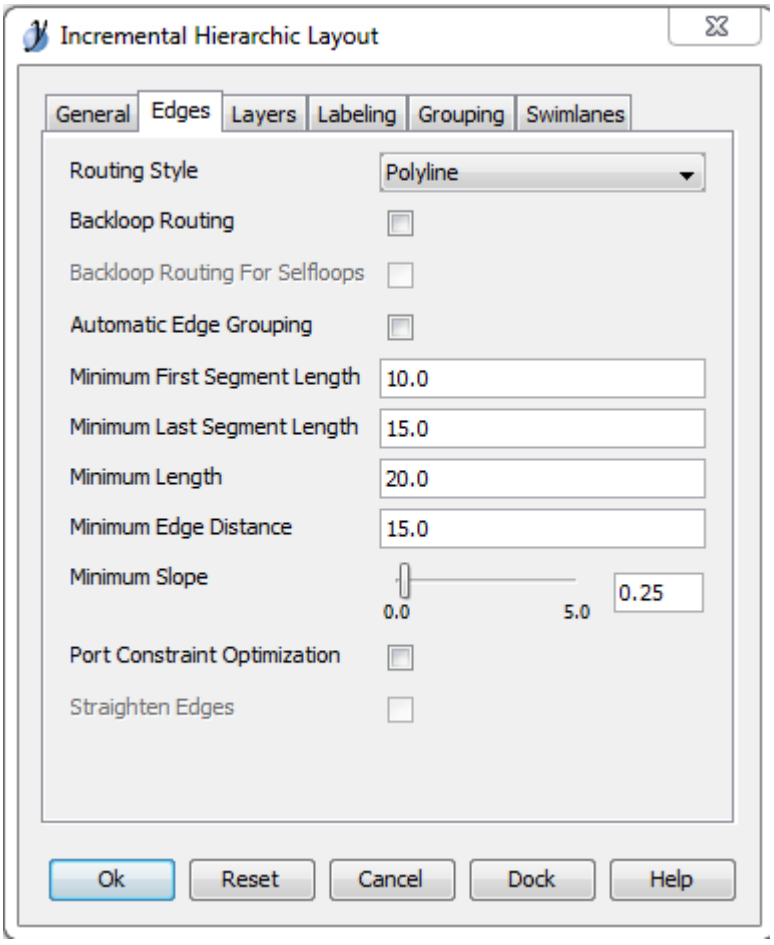



**Figure 7-13 Configuring Routing Style in yEd Graph Editor**

3 Click **Ok.**

When you open the <file name>_logicpath.gml file in yEd Graph Editor, initially you might see many rectangle boxes overlapping each other or a single rectangle box as shown in the following example.

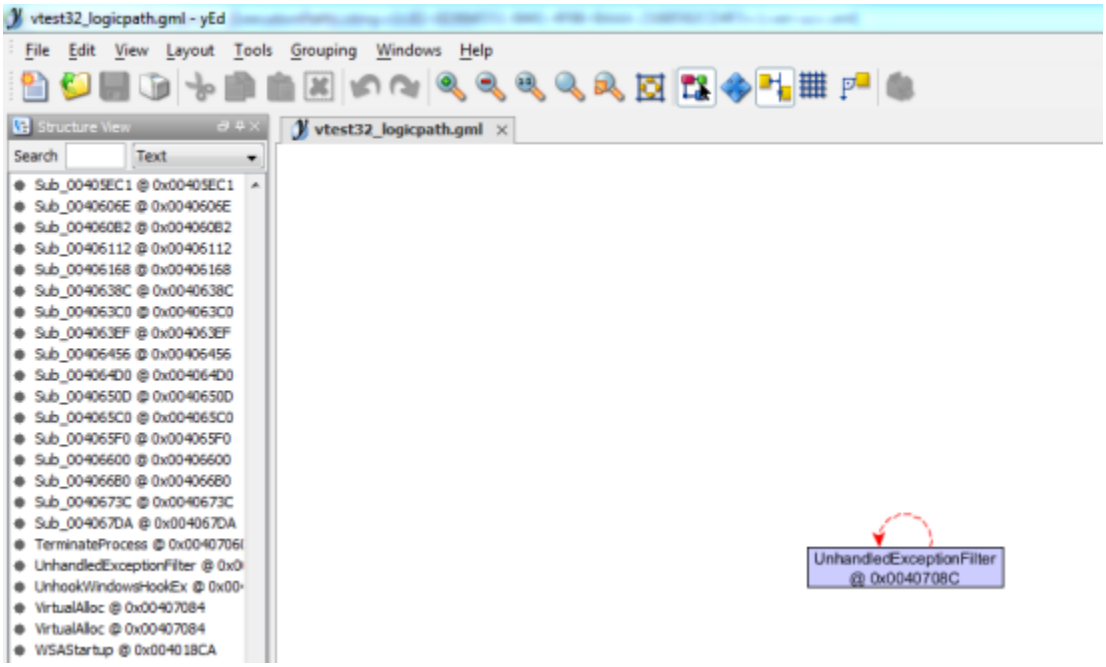



**Figure 7-14 Open <file name>_logicpath.gml file**

In the yEd Graph Editor select **Layout** | **Hierarchical.**

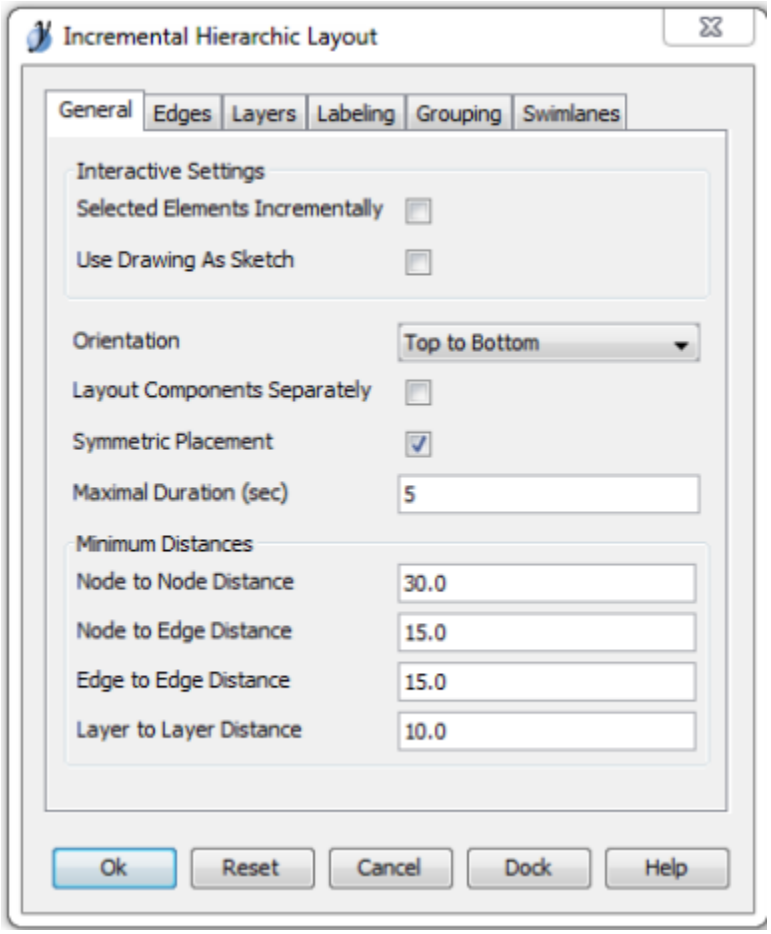



**Figure 7-15 Incremental Hierarchic Layout dialog**

In the **Incremental Hierarchic Layout** dialog, click **Ok** without changing any of the default settings. The following example shows the complete layout of the relationship of all subroutines detected during static disassembly processed.

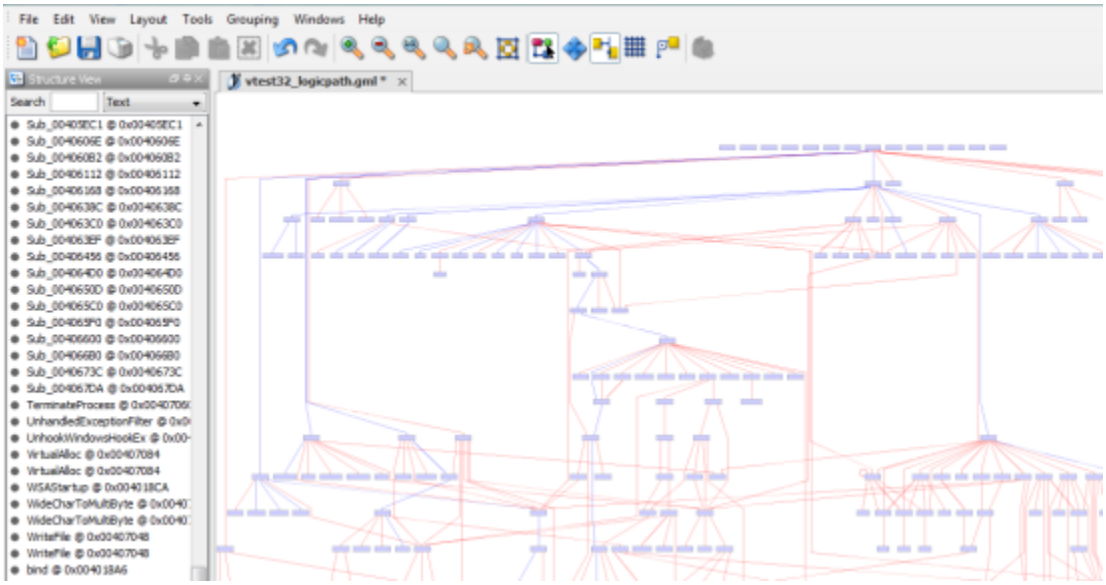



**Figure 7-16 Layout of the subroutines relationships**

The graph depicts an overview of the complexity of the sample as seen by the cross-reference of function calls. The following shows more detail on the function names and their addresses as seen by zooming in.

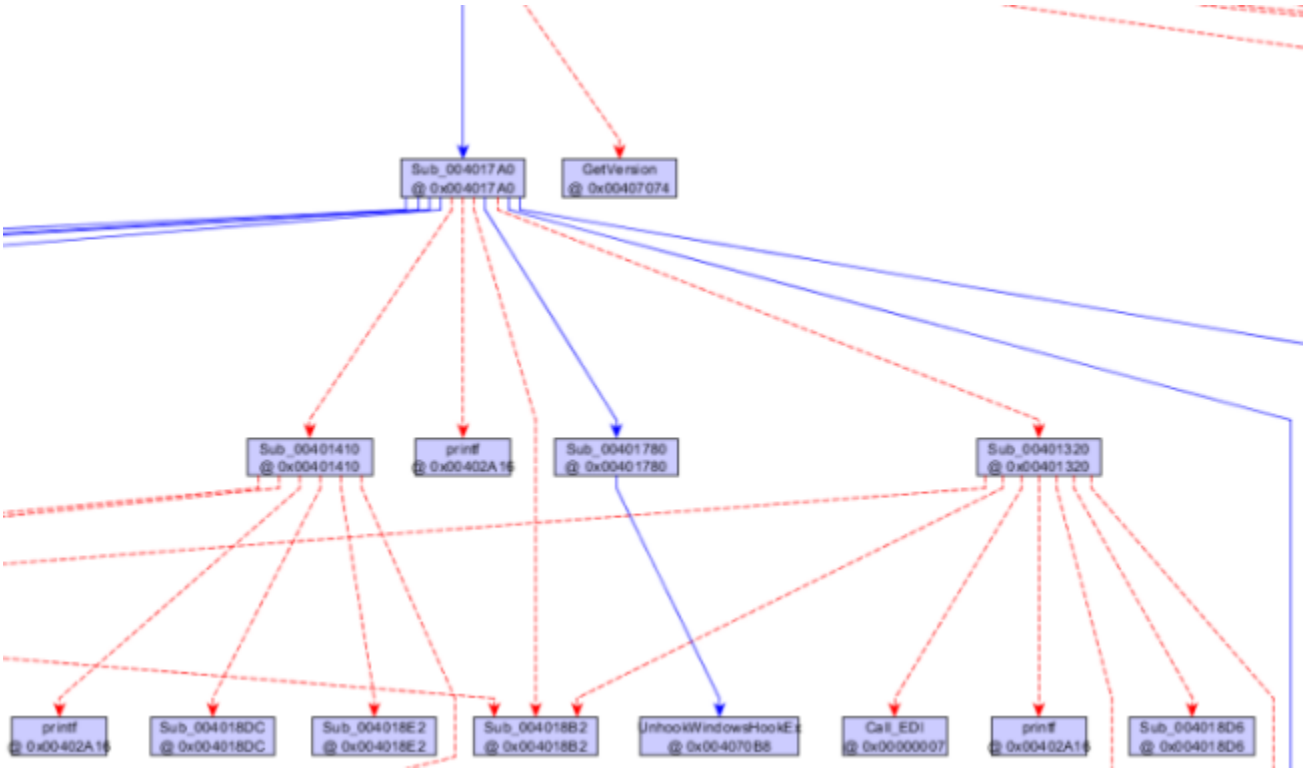



**Figure 7-17 Zoom in on the layout**

Two colors are used to indicate the executed path. The red dash lines show the non-executed path, and the blue solid lines show the executed path.

According to the preceding control graph, the subroutine (Sub_004017A0) at virtual address 0x004017A0 was executed and is shown with a blue solid line pointing to the Sub_004017A0 box. However, the subroutine (GetVersion]) was not called potentially as there is a red dash line pointing to it.

The Sub_004017A0 subroutine is making 11 calls as there are 11 lines coming out of this box. Seven of these 11 calls were executed during dynamic analysis. One of them is calling Sub_00401780 as there is a blue solid line pointing from Sub_004017A0 to Sub_00401780. Calls to Sub_00401410, printf, Sub_00401882, and Sub_00401320 were not executed and shown with red dashed line pointing at them.

The Sub_00401780 subroutine is making only one unique call as there is only one line coming out from this box. This call was executed during dynamic analysis.

## User API Log

The User API Logs are contained in various files.

- The .log file contains the Windows user-level DLL API calls made directly by the analyzed file during dynamic analysis. To view this file in the McAfee Advanced Threat Defense web application, select **Analysis** | **Analysis Results**. Then click and select **User API Log**. Alternatively, click , select **Complete Results**. Download the <sample_name>.zip file. This .zip file contains the same information in the <sample name>.log file in the AnalysisLog folder. The content of the .log file includes the following:
  - A record of all systems DLL API calling sequence.
  - An address which indicates the approximate calling address where the DLL API call was made.
  - Optional input and output parameters, and return code for key systems DLL API calls.
- The following are the other files containing the dynamic execution logs. All these files are contained in the <sample name>.zip file.
  - <sample name>ntv.txt file. This file contains the Windows Zw version of native system services API calling sequence during the dynamic analysis. The API name typically starts with Zw as in ZwCreateFile.
  - log.zip
  - dump.zip
  - dropfiles.zip
  - networkdrive.zip

## Download the complete results .zip file

McAfee Advanced Threat Defense produces detailed analysis for each submitted sample. All the available reports for an analyzed sample are available in a .zip file, which you can download from the McAfee Advanced Threat Defense web application.

### Task

1 Select **Analysis** | **Analysis Results**.

2 In the **Analysis Results** page, click and select **Complete Results** .

Download the <sample_name>.zip file to the location you want. This .zip file contains the reports for each analysis. The files in this .zip file are created and stored with a standard naming

convention. Consider that the sample submitted is vtest32.exe. Then the .zip file contains the following results:

- vtest32_summary.html (.json, .txt, .xml) — This is the same as the Analysis Summary report. There are four file formats for the same summary report in the .zip file. The html and txt files are mainly for end users to review the analysis report. The .json and .xml files provide well-known malware behavior tags for high-level programming script to extract key information.

  If the malware severity is 3 and above, then it contains .ioc, and .stix.xml formats of the Analysis Summary report for the sample.

- vtest32.log — This file captures the Windows user-level DLL API calling activities during dynamic analysis. You must thoroughly examine this file to understand the complete API calling sequence as well as the input and output parameters. This is the same as the User API Log report.
- vtest32ntv.txt — This file captures the Windows native services API calling activities during dynamic analysis.
- vtest32.txt — This file shows the PE header information of the submitted sample.
- vtest32_detail.asm — This is the same as the Disassembly Results report. This file contains reverse-engineering disassembly listing of the sample after it has been unpacked or decrypted.
- vtest32_logicpath.gml — This file is the graphical representation of cross-reference of function calls discovered during dynamic analysis. This is the same as the Logic Path Graph report.
- log.zip —This file contains all the run-time log files for all processes affected by the sample during the dynamic analysis. If the sample generates any console output text, the output text message is captured in the ConsoleOutput.log file zipped up in the log.zip file. Use any regular unzip utility to see the content of all files inside this log.zip file.
- dump.zip — This file contains the memory dump (dump.bin) of binary code of the sample during dynamic analysis. This file is password protected. The password is *virus*.
- dropfiles.zip — This is the same as the Dropped Files report in the **Analysis Results** page. The dropfiles.zip file contains all files created or touched by the sample during the dynamic analysis. It is also password protected. The password is *virus*.

McAfee Advanced Threat Defense does not provide you access to the original sample files that it analyzed. If Network Security Platform is integrated, you can use the **Save File** option in the Advanced Malware policy to archive samples. However, note that the Sensor's simultaneous file scan capacity is reduced if the **Save File** option is enabled. See the latest *Network Security Platform IPS Administration Guide* for the details.

# Working with the McAfee Advanced Threat Defense Dashboard

When you access McAfee Advanced Threat Defense from a client browser, the McAfee Advanced Threat Defense Dashboard is displayed. You can view the following monitors on the McAfee Advanced Threat Defense Dashboard:

- VM Creation Status — Shows the status for analyzer VMs that being created.
- File Counters — Provides a status of files being analyzed.
- Files analyzed by File Type — Provides a view of file types being analyzed.
- Top Malware by File Name — Lists the most severe malware files in your network by file name.
- Analyzer Profile Usage — Provides the details of the analyzer profiles being used.

- System Health — Provides the system health details of the McAfee Advanced Threat Defense Appliance.
- System Information — Provides the version numbers for the software components of McAfee Advanced Threat Defense Appliance.

### Task

1 Click **Dashboard** to view the monitors.

2 Specify the criteria for the data to be displayed in the monitors.

a Specify the time period for the information to be displayed in the monitors.

For example, you can select to view the information for the past one hour. By default, data for the past 14 days is shown. This field does not affect the System Health and System Information monitors.

b To refresh the monitors now, click .

c Click to edit the dashboard settings.

**Table 7-12 Dashboard settings**

| Option | Definition |
|---|---|
| **Monitors** | Select the monitors that you want to see on the Dashboard. |
| **Automatic Refresh** | Set the frequency at which the Dashboard should automatically refresh itself.<br>If you want to refresh the dashboard only manually, select **Disabled**. When required to refresh the Dashboard, click . This enables you to view the snapshot of the Dashboard at a specific point in time. |
| **Layout** | Specify the number of columns into which you want to organize the Dashboard. |
| **OK** | Click to save and apply the Dashboard settings. |
| **Cancel** | Click to retain the last saved settings. |

3 Optionally, set the display settings for each monitor.

- To collapse a monitor, click
- To hide a monitor, click
- To change the display format of a monitor, click

## Malware analysis monitors

The following are the monitors related to malware analysis.

## File Counters

This monitor shows the analysis status for files submitted during the specified time period. For example, if you set the time period for the data in the dashboard as last 5 minutes, this monitor shows the count of files in completed, analyzing, and waiting statuses since the last 5 minutes. If you view this monitor in the stacked bar chart format, it also displays the severity level for the files.

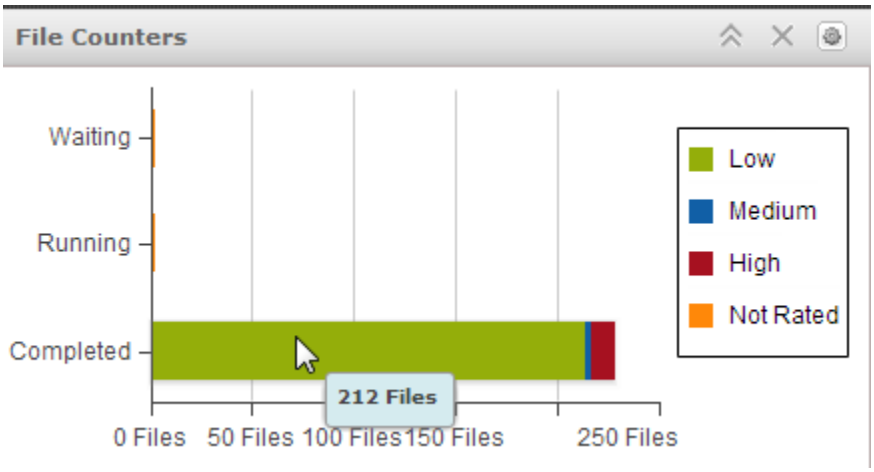



**Figure 7-18 File Counters monitor**

- The confidence levels are indicated using various colors.
- To hide the files for a particular confidence level, click the corresponding confidence level in the legend. For example, if you want to focus on only the high severity files, click **Low** and **Medium** in the legend. Now the chart shows only the high-severity malware that is in the waiting, running, and completed statuses. Click again on **Low** and **Medium** to view the combined chart.
- Move the mouse over a particular block in the chart to view the number of files that make up that block.

## Files analyzed by File Type

This monitor shows the count of files analyzed against their type. In the tabular format, it shows the percentage for each type. In the chart, it also shows the count of infected and non-infected files.

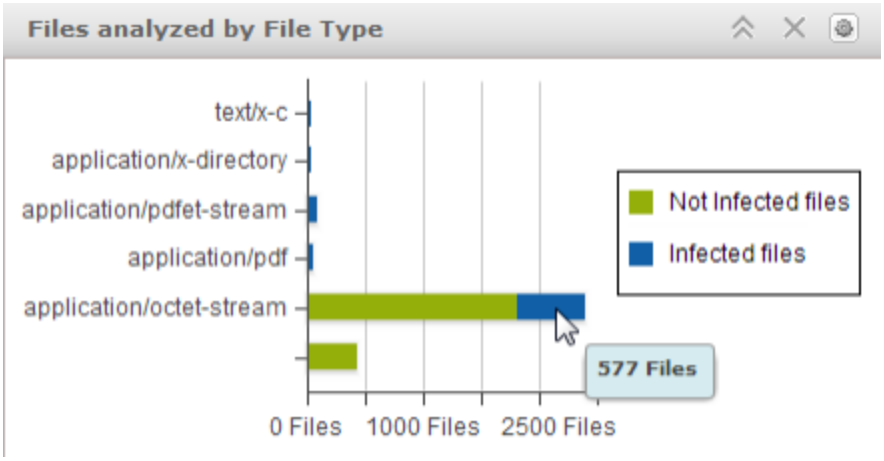



**Figure 7-19 Files analyzed by File Type monitor**

- The infected and not infected file counts are indicated using different colors.
- To hide the infected or not infected files, click the corresponding confidence level in the legend.
- Move the mouse over a particular block in the chart to view the number of files that make up that block.

## Analyzer Profile Usage

This monitor shows the number of times each analyzer profile has been used for analyzing files.

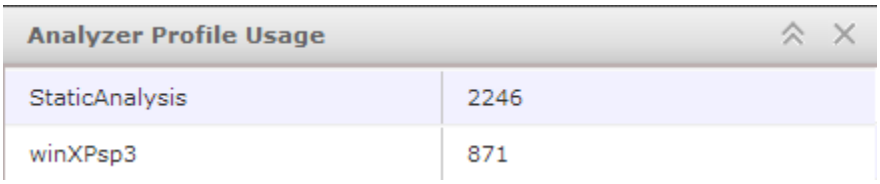



**Figure 7-20 Analyzer Profile Usage monitor**

## Top malware by file name

In this monitor, you can view the names of the malicious files detected in your network with the most severe ones listed on top. This information might enable further research such as finding more information about these files on the web.

- The listed malware files are sorted based on their severity score in the descending order. This score is displayed in the second column. The following are the severity scores:
  - 5 — Very high severity
  - 4 — High severity
  - 3 — Medium severity
  - 2 — Low severity
  - 1 — Very low severity
  - 0 — Informational severity (white-listed files)
- The first column displays the file names. Files of the same severity are sorted in the alphabetical order.

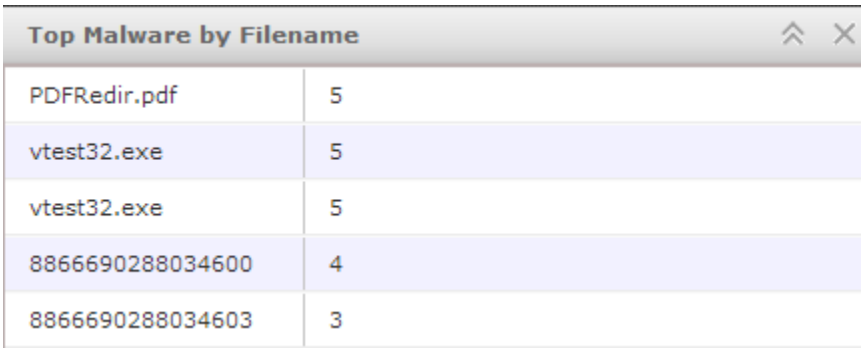



**Figure 7-21 Top Malware by File Name monitor**

## VM Creation Status monitor

This monitor displays the status of the analyzer VMs created for the specified time period in the dashboard. For example, if you specified *Last 12 hours*, this monitor shows the status of analyzer VMs that were created in the last 12 hours.

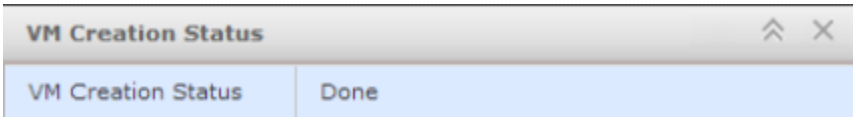



**Figure 7-22 VM Creation Status monitor**

## McAfee Advanced Threat Defense performance monitors

The following are the monitors related to McAfee Advanced Threat Defense Appliance performance.

### System Health

This monitor displays the health of the McAfee Advanced Threat Defense Appliance in a table.

- System Health — Indicates whether the system health is in good state.
- DNS Status — Indicates the connection status between Advanced Threat Defense and the configured DNS servers. If Advanced Threat Defense is able to connect to the preferred and alternate DNS server, then the DNS Status is *healthy.* If Advanced Threat Defense is unable to connect to the preferred DNS server, the DNS Status is *critical.*
- Uptime — The number of hours the Appliance has been running continuously.
- CPU Load — The actual system load. For example, 100% CPU load indicates the CPU is fully loaded; 125% indicates that the CPU is fully loaded and 25% of the load is yet to be processed.
- Memory Utilization — The percentage of the Appliance's memory in use currently.
- Data Disk Space — The Appliance's disk capacity (in terabyte) for sample data storage such as the samples themselves and their report files.
- Data Disk Available — Disk space currently available (in terabyte) for sample data storage.

| System Health | |
|---|---|
| System Health | Good |
| Uptime | 6 days |
| CPU Load | 3.5% |
| Memory Utilization | 4.49% |
| Data Disk Space | 3.02T |
| Data Disk Available | 2.77T |
| System Disk Space | 63G |
| System Disk Available | 27.55G |

**Figure 7-23 System Health monitor**

- System Disk Space — The Appliance's disk capacity for storing the McAfee Advanced Threat Defense system software data.
- System Disk Available — Disk space currently available for storing the McAfee Advanced Threat Defense system software data.

## System Information

This monitor shows the version numbers of the software components related to McAfee Advanced Threat Defense.

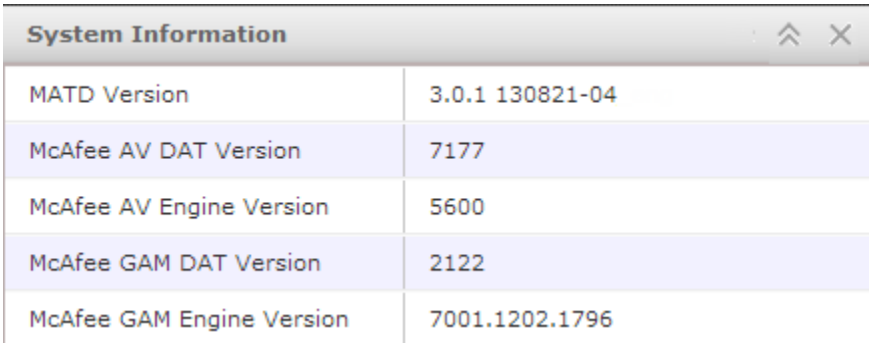



**Figure 7-24 System Information monitor**

# 8 Clustering McAfee Advanced Threat Defense Appliances

When you have a very heavy load of files to be analyzed for malicious content, you can cluster two or more McAfee Advanced Threat Defense Appliances. So, the analysis load is efficiently balanced between the McAfee Advanced Threat Defense Appliances (nodes) in the cluster.

Consider multiple inline Sensors submitting hundreds of files per second to one McAfee Advanced Threat Defense Appliance. In the blocking mode, a Sensor waits for up to 6 seconds for McAfee Advanced Threat Defense to analyze a file. After this time period, the Sensor forwards the file to the target endpoint. Faster response from McAfee Advanced Threat Defense could be accomplished by clustering McAfee Advanced Threat Defense Appliances for load-balancing.

**Contents**


- *Understanding McAfee Advanced Threat Defense cluster*
- *Pre-requisites and considerations*
- *Network connections for an Advanced Threat Defense cluster*
- *How the Advanced Threat Defense cluster works?*
- *Configuring an Advanced Threat Defense cluster - high-level steps*


## Understanding McAfee Advanced Threat Defense cluster

Clustering McAfee Advanced Threat Defense Appliances is a feature, which is available from release 3.2.0. To create a cluster of McAfee Advanced Threat Defense Appliances, you need two or more functional McAfee Advanced Threat Defense Appliances. Among these McAfee Advanced Threat Defense Appliances, identify the primary McAfee Advanced Threat Defense Appliance. All other McAfee Advanced Threat Defense Appliances act as the secondary. You use the web application of the primary node to integrate these McAfee Advanced Threat Defense Appliances to form the cluster. Each McAfee Advanced Threat Defense Appliance in a cluster is referred to as a node.

The primary node or the primary McAfee Advanced Threat Defense Appliance acts as the external interface for the cluster. That is, the primary node's IP address acts as the cluster's IP address from the standpoint of configuration and file submission. The integrated products and users access the primary node to submit files for analysis and retrieve the results and reports. The primary node is also the template and control center for the cluster. It is responsible for load-balancing the files among all nodes and for retrieving the reports of analyzed files.

As mentioned earlier, clustering McAfee Advanced Threat Defense Appliances serves to load-balance the files and provides a high-availability of secondary nodes.

If the primary node is down for some reason, the entire cluster is down. The primary node is not replaced by a secondary node at any point unless you reconfigure the cluster itself.

# Pre-requisites and considerations

- There can be a maximum of 10 nodes in a cluster including the primary node.
- It is recommended that you use the eth-0 interfaces (management ports) of the McAfee Advanced Threat Defense Appliances for cluster communication. Also, for best performance, the eth-0 interfaces of all nodes must be in the same layer-2 network.

  To locate the eth-0 interfaces in your Appliance, see Check your shipment on page 20.
- The nodes must be homogenous regarding the following:
  - McAfee Advanced Threat Defense software version. The software versions of all nodes must exactly match.
  - Analyzer VMs. All nodes must have the same analyzer VMs.

    Before you configure the cluster, make sure the VM profiles are exactly the same in all the nodes of the cluster. All the settings in the VM profiles, including the VM profile name, must be the same across the nodes.

    When you create a new VM profile or modify an existing one after cluster-creation, recall that VM-profile-related changes are not propagated to all the nodes automatically. First, dismantle the cluster. Then manually make the exact change in each node. If you are creating a new VM profile, make sure you create this VM profile in all the nodes before you select this new VM profile in any of the analyzer profiles. If you need to modify an existing VM profile, make sure you immediately do the same modification in each node. Finally, recreate the cluster.
  - VM profiles on all nodes must exactly match.
  - It is recommended that DAT and engine versions of McAfee Anti-Malware Engine are the same in all nodes.
  - It is recommended that DAT and engine versions of McAfee Gateway Anti-Malware Engine are the same in all nodes.
- The nodes can be heterogenous regarding the following:
  - Hardware. That is, you can create a cluster using a combination of ATD-3000 and ATD-6000 Appliances.
  - FIPS compliance. Regardless of primary or secondary, some nodes can be in FIPS mode and the rest in non-FIPS mode.
- Use the IP address of the primary node to submit files and to integrate with other products such as Network Security Platform and Web Gateway.

  If you integrate Network Security Platform and Web Gateway with the secondary nodes, these nodes function like standalone McAfee Advanced Threat Defense Appliances.
- If the primary node is down, the entire cluster goes down.
- Integrating an McAfee Advanced Threat Defense cluster with Email Gateway is not supported.
- Currently, there is no consolidated display of analysis status and analysis results for a cluster. That is, you can view the analysis status and analysis results for files analyzed by each node separately.

# Network connections for an Advanced Threat Defense cluster

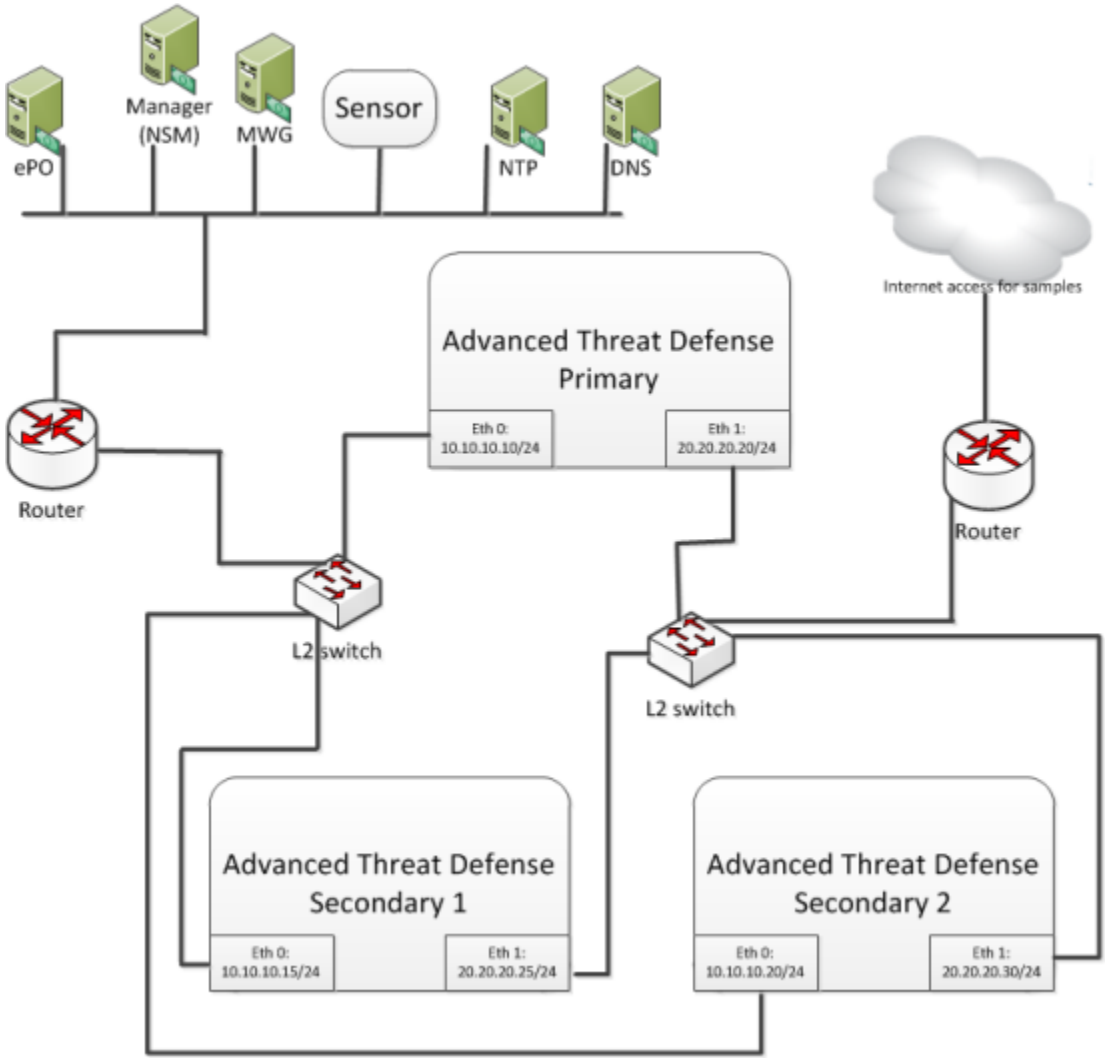



**Figure 8-1 An example Advanced Threat Defense cluster deployment**

In the example illustrated above, the eth-0 interfaces of all nodes are connected to the same switch (L2 network). Eth-0 interface of the primary acts as the management interface of the cluster whereas the eth-0 of the secondary are used to exchange information with the primary. The primary node load balances the files received on the eth-0 interface among the secondary nodes in a round-robin fashion. It transfers files to be analyzed by the secondary node through the eth-0 interface and uses the same to retrieve results. When cluster configuration changes are made using the primary node, they are synchronized across the secondary nodes through the eth-0 interface.

In this example, eth-1 is used to provide network access to malware running on the analyzer VMs. This isolates the network traffic generated by malware from the production network to which eth-0 interfaces are connected.

# How the Advanced Threat Defense cluster works?

Recall that when you cluster Advanced Threat Defense Appliances, the primary node acts as the template and control center for the entire cluster. After you define the cluster, you use the primary node to manage the configuration for the cluster.

For the sake of explanation, the entire Advanced Threat Defense configuration can be classified as the following:

- Synchronized configuration — Certain configurations can only be done using the primary node. When you save these configurations, the primary node sends a snapshot of its current configuration as a file to all secondary nodes. The secondaries save these settings in their database. This synchronization process does not affect the file analysis capabilities of an Advanced Threat Defense Appliance.

  The primary node has the latest version of the configuration file. If the version of the configuration file does not match between the primary and a secondary node, the primary node pushes the configuration file automatically to that secondary.

  The following configurations are synchronized automatically between all nodes:

  - Analyzer profiles
  - User management
  - McAfee ePO integration details
  - HTTP proxy settings
  - DNS settings
  - System time based on the settings in the **Date and Time Settings** page. If you manually modify the time, the same is set on all nodes. If you configure NTP servers, the same NTP servers are used for all nodes. However, time zone is not synchronized.

  The web application pages for the configurations listed above are disabled in the secondary nodes.

- Unsynchronized configuration — The following are not synchronized automatically. Use the individual nodes to configure these.
  - Advanced Threat Defense software version.
  - Analyzer VMs.

    Before you configure the cluster, make sure the VM profiles are exactly the same in all the nodes of the cluster. All the settings in the VM profiles, including the VM profile name, must be the same across the nodes.

    When you create a new VM profile or modify an existing one after cluster-creation, recall that VM-profile-related changes are not propagated to all the nodes automatically. First, dismantle the cluster. Then manually make the exact change in each node. If you are creating a new VM profile, make sure you create this VM profile in all the nodes before you select this new VM profile in any of the analyzer profiles. If you need to modify an existing VM profile, make sure you immediately do the same modification in each node. Finally, recreate the cluster.

  - VM profiles.
  - DAT and engine versions of McAfee Anti-Malware Engine.
  - DAT and engine versions of McAfee Gateway Anti-Malware Engine.

- Whitelist and blacklist entries.
- Time zone.
- In a Advanced Threat Defense cluster setup, each node maintains its set of custom YARA rules. That is, the custom YARA rules that you define in the primary node are not sent to the secondary nodes automatically.

> Configuration changes made through the CLI are not exchanged. Make the same changes in each node individually.

When treated as part of a cluster, the secondary nodes are transparent to users and integrated products.

- It is possible for you to use a secondary Advanced Threat Defense directly for file submission and report retrieval. However, you are not allowed to modify any of the synchronized configurations.
- Both files and URLs submitted for analysis are distributed to achieve load-balancing.

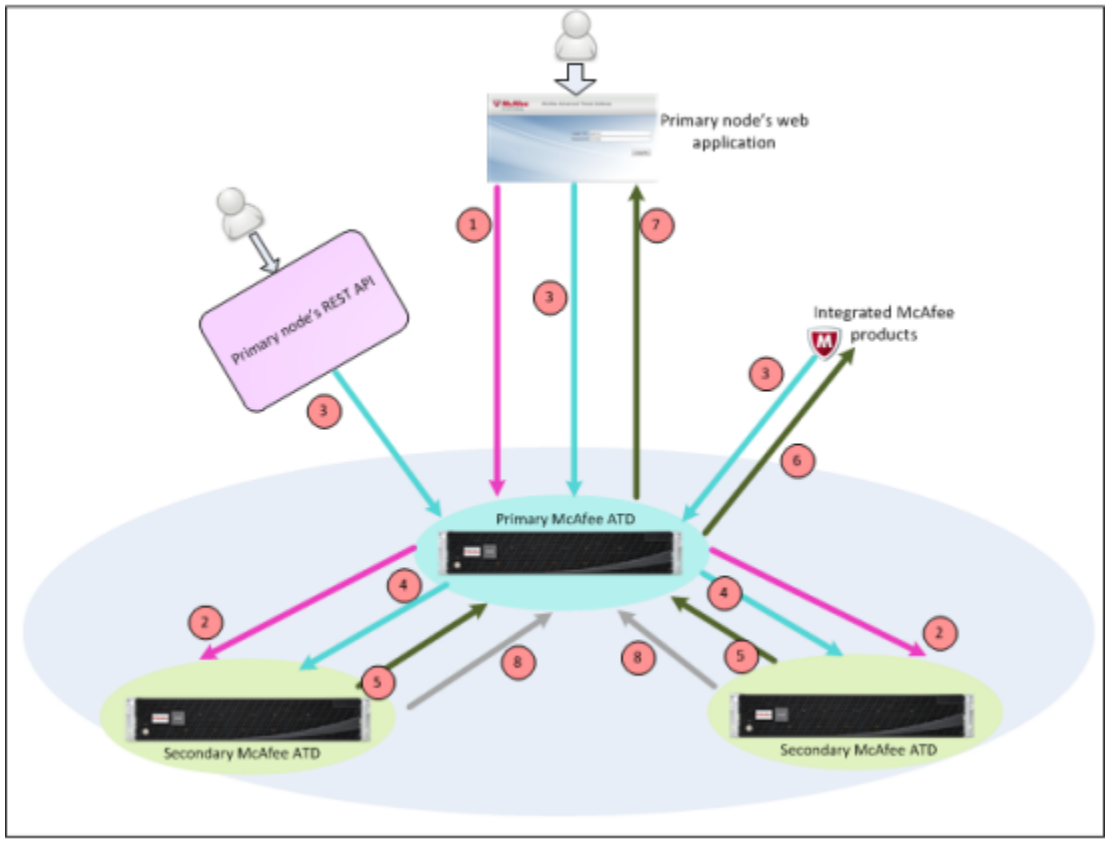



**Figure 8-2 Advanced Threat Defense Appliances in a cluster**

| Callout number | Legend | Description |
|---|---|---|
| 1 | | You access the primary node's web application to modify the synchronized configurations. |
| 2 | | When you save the configuration changes, the primary node pushes the current configuration to all secondary nodes. So, all nodes have the same synchronized configuration. |

| Callout number | Legend | Description |
|---|---|---|
| 3 | | File submission to the cluster happens through the following methods:<br>• You submit files for analysis using the primary node's web application.<br>• File submission to the primary node through its REST APIs.<br>• The McAfee products integrated with the Advanced Threat Defense submit files for analysis. |
| 4 | | The primary node distributes the files among the member nodes (including the primary itself). |
| 5 | | Integrated McAfee products such as the Network Security Manager query the primary node for analysis reports. Also, the primary node displays the status and results of all files analyzed by the cluster. For these reasons, the primary node pulls the analysis results from the secondary nodes. |
| 6 | | The primary node provides the reports to the integrated McAfee products. |
| 7 | | You can view the analysis status and the results of all files analyzed by the cluster from the primary node. From the primary node, you can also view the analysis reports of any file that you directly submitted to a secondary node. |
| 8 | | At regular intervals, the secondary nodes send a heartbeat signal to the primary to indicate the secondary's health and status. |

## How are the individual files in a .zip file analyzed by an Advanced Threat Defense cluster?

When you submit a file or URL, Advanced Threat Defense assigns it a unique job ID and a task ID. These IDs are incremental integers. When you submit a .zip file, the component files are extracted and analyzed separately. The job ID for all component files of a .zip file is the same as that of the .zip file's job ID. However, the task ID varies for each component file.

When you submit a .zip file to an Advanced Threat Defense cluster, the primary node identifies the node to which it should distribute the next file and sends the entire .zip file to that node. The node that received the .zip file extracts the component files and analyses them. This applies to .zip files within a .zip file as well.

- If a Sensor submits the .zip file, Advanced Threat Defense generates a cumulative report for the entire .zip file. That is, one report for one .zip file is sent to the Manager when it queries for the report. In case of Web Gateway, .zip files are not supported.
- If you submit a .zip file to the primary node, using its web application for example, individual reports are generated for the component files in the .zip file.

Then the primary node extracts the component files in the zip and distributes them all to the same node for analysis. The primary polls the corresponding secondary for analysis status and results using unique task ID.

### How to upgrade the Advanced Threat Defense software for the nodes in a cluster?

Following is the recommended procedure to upgrade the Advanced Threat Defense software for the nodes in a cluster :

1. If you upgrade the primary first, then the entire cluster breaks. Therefore, you can begin with upgrading the secondary nodes. When a secondary node's software version is upgraded, the primary does not distribute files to that secondary.
2. After you upgrade more than 50percent of the secondary nodes, upgrade the primary node. The primary does not distribute files to the secondary nodes that are on the earlier version.
3. Upgrade the remaining secondary nodes.

Do not select **Reset Database** when you upgrade any of the nodes. If this option is selected for the primary node, the cluster goes down after upgrade. If the **Reset Database** option is selected for a secondary node, it breaks away from the cluster after upgrade.

If you downgrade the primary node, the cluster breaks. To downgrade a secondary, remove that secondary node from the cluster and downgrade it to the required version.

## Process flow for Network Security Platform

Consider a scenario where a Sensor is inline between the endpoints on your network and the Web. This Sensor is integrated with a Advanced Threat Defense cluster consisting of 3 Advanced Threat Defense Appliances.

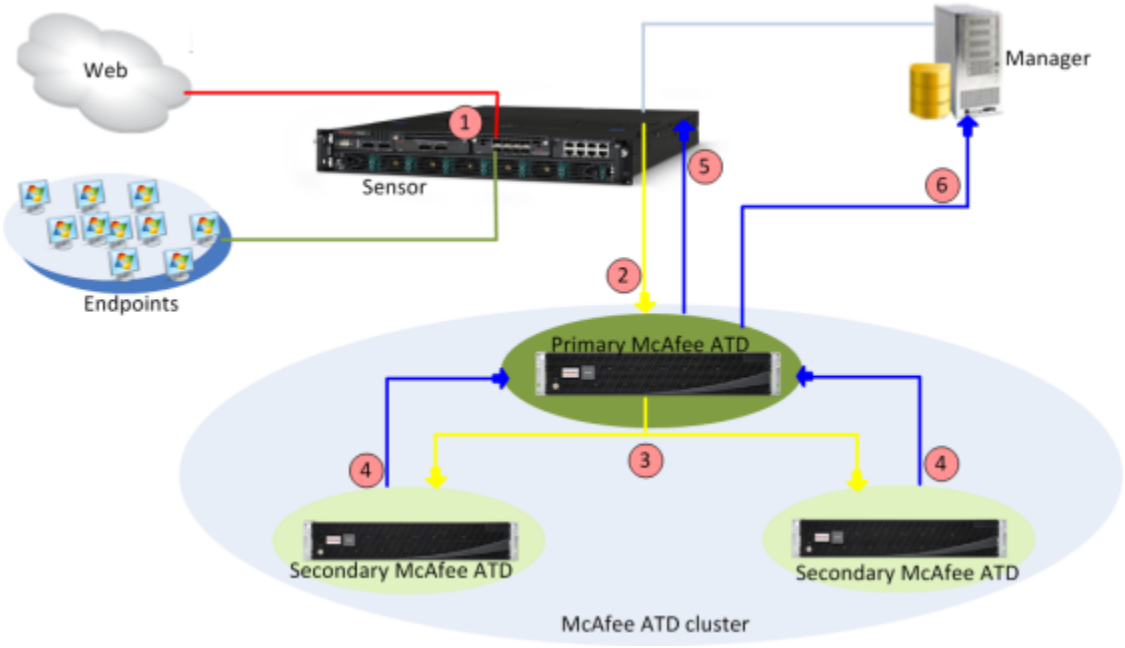



**Figure 8-3 Network Security Platform integrated with an Advanced Threat Defense cluster**

| Number | Description |
|---|---|
| 1 | The endpoints attempt to download files from the Web. The inline monitoring ports detect this activity. |
| 2 | For a given file, the Sensor withholds the last packet from being forwarded to the endpoint and simultaneously streams the file packets to the primary Advanced Threat Defense for analysis. For this purpose, the Sensor and the primary Advanced Threat Defense use their management ports. |

| Number | Description |
|---|---|
| 3 | After the entire file is with the primary Advanced Threat Defense, it distributes this file to one of the Appliances in the cluster. Assume that the file is sent to one of the secondary Advanced Threat Defense Appliances. For all communication, the members in the cluster use their management ports. |
| 4 | The corresponding secondary Advanced Threat Defense responds with a job ID to the primary and begins to analyze the file based on the *nsp* user profile. If the file is detected by static analysis, the secondary Advanced Threat Defense sends the malware result (severity) to the primary Advanced Threat Defense. |
| 5 | • If the file is detected by static analysis, the primary Advanced Threat Defense sends the malware result that it received from the secondary Advanced Threat Defense to the Sensor's management port.<br>• If the file is dynamically analyzed, the Sensor raises an informational alert in the Real-time Threat Analyzer. This informational alert is set to auto-acknowledge by default, which you can disable if necessary. |
| 6 | The Sensor forwards the job ID to the Manager. The Manager queries the primary Advanced Threat Defense Appliance management port for the analysis reports. The primary Advanced Threat Defense pulls the reports from the corresponding Advanced Threat Defense Appliance based on the job ID. Then it forwards the reports to the Manager for display. Also, if the file is found to be malicious based on dynamic analysis, the alert in the Real-time Threat Analyzer is updated accordingly. |

## Process flow for McAfee Web Gateway

Consider a scenario where Web Gateway is inline between the endpoints on your network and the Web. This Web Gateway Appliance is integrated with a Advanced Threat Defense cluster consisting of three Advanced Threat Defense Appliances.

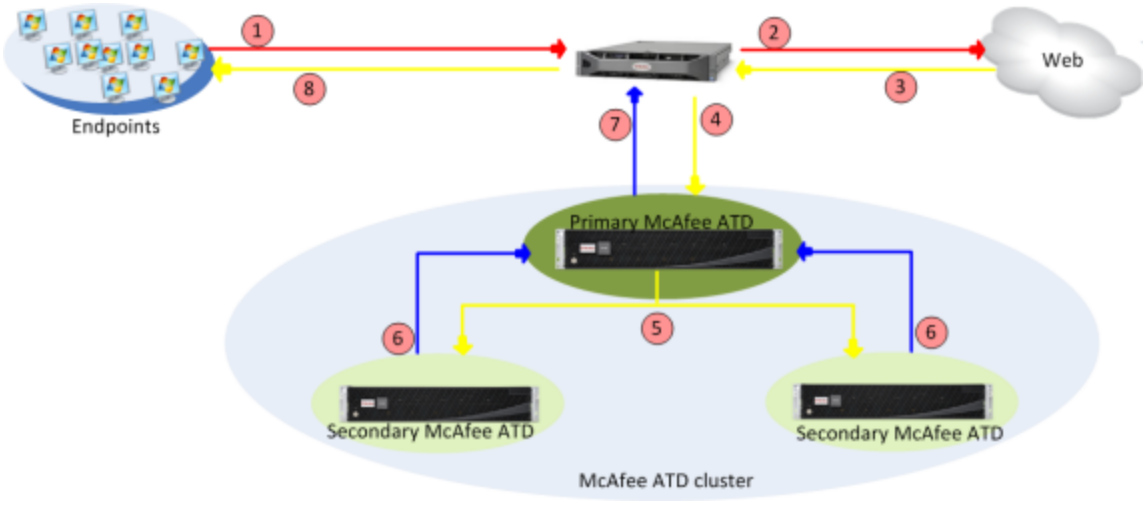



**Figure 8-4 Web Gateway integrated with an Advanced Threat Defensecluster**

| Number | Description |
|---|---|
| 1 | The endpoints attempt to download web objects. |
| 2 | Web Gateway forwards these requests. |
| 3 | When a file is downloaded, the native McAfee Gateway Anti-malware Engine on Web Gateway scans the file and determines the malware score. |
| 4 | Based on the file type and the malware score, Web Gateway determines if the file needs to be sent to Advanced Threat Defense for analysis and, if needed, forwards the file to the primary Advanced Threat Defense's management port. |

| Number | Description |
|---|---|
| 5 | The primary Advanced Threat Defense distributes such files among the members based on round-robin. All communication between the members in a cluster is over their management ports.<br>Assume that the file is sent to one of the secondary Advanced Threat Defense for analysis. The secondary Advanced Threat Defense returns the job ID and task ID to the primary node and begins to analyze the file. The primary node, in turn, returns the job ID and task ID to Web Gateway. |
| 6 | For the analysis reports, Web Gateway queries the primary node with the task ID. Using the task ID, the primary node identifies the Advanced Threat Defense that analyzed the file and pulls the reports from it. |
| 7 | In response to the query from Web Gateway, the primary Advanced Threat Defense forwards the reports. |
| 8 | Based on the report from Advanced Threat Defense, Web Gateway allows or blocks the file accordingly. |

**Notes:**

- When Web Gateway queries for an MD5 hash value with time period (without the job or task ID), the primary node checks the MD5 hash in its database. If there is no matching record, the primary node checks the secondary nodes where the file is analyzed and sends the report back to Web Gateway without analyzing the corresponding file again.
- When Web Gateway queries for an MD5 hash value for a running task (without the job or task ID), the primary node checks the MD5 hash with status (waiting or analyzing) in its database. If there is no matching record, the primary node checks the secondary nodes where the file is being analyzed or is in the queue. Then the primary node sends the task details back to Web Gateway without analyzing the corresponding file again.

# Configuring an Advanced Threat Defense cluster - high-level steps

Follow these high-level steps to configure an Advanced Threat Defense cluster.

1. Identify the Advanced Threat Defense Appliances that you want to use to create the cluster. You can add additional secondary nodes to a working Advanced Threat Defense cluster.
2. Make sure that the Advanced Threat Defense Appliances meet the requirements as discussed in Pre-requisites and considerations on page 282.
3. Out of the Advanced Threat Defense Appliances, identify the one that you plan to use as the primary node. All other Advanced Threat Defense Appliances are secondary nodes. Once you define the cluster, you cannot change the primary node without redefining the cluster itself.

   Factor in the following when you decide on the primary node.

   - Use the primary node's IP address to submit files and to manage the configuration.
   - Products such as Network Security Platform and Web Gateway must be integrated with the primary node's IP address. Since the result and report retrieval is through the primary, connection between the integrated products and the secondary nodes is not mandatory.

- Make sure the analyzer VMs and VM profiles are identical across all nodes.

  If you require to add an analyzer VM or if you require to add, modify, or delete a VM profile, break the cluster, make the required changes in all nodes, and then re-create the cluster.

- The synchronized configurations of the secondary are overwritten with that of the primary node. Post cluster creation, you use the primary node to manage these configurations. For information on synchronized configurations, see How the Advanced Threat Defense cluster works? on page 284.

4 Make sure the secondary nodes and the primary node are able to communicate with each other using their management ports.

5 As a best practice, back up the configuration of all nodes, especially the secondary nodes, before you configure the cluster.

6 Make sure that the integrated products are configured to use the primary node. This includes the integrated McAfee products as well as any third-party application or script that use the Advanced Threat Defense REST APIs.

7 Create the McAfee Advanced Threat Defense cluster on page 290.

8 Submit files and URLs to the Advanced Threat Defense cluster.

9 View the analysis results for an Advanced Threat Defense cluster.

10 Manage configurations for the cluster.

# Create the McAfee Advanced Threat Defense cluster

**Before you begin**

- You have reviewed Configuring an Advanced Threat Defense cluster - high-level steps on page 289.
- You have admin-user rights for the primary node's web application.
- The primary and secondary nodes are not part of any other cluster.
- The software version (active version) of all nodes that you plan to use are an exact match.

## Task

1 Identify an Advanced Threat Defense Appliance as the primary node and log on to its web application.

Use a user name that has admin rights.

2 Select **Manage** | **Load Balancing**.

The **Load Balancing Cluster Setting** page displays.

3 In the **Node IP address** field, enter the management port IP address of the primary node and click **Add Primary Node**.

4 Confirm if you want to create the cluster.

Advanced Threat Defense sets itself as the primary node for the cluster.

5 In the **Node IP address** field, enter the management port IP address of a secondary node and click **Add Secondary Node**.

6 Click **Yes** to add the secondary node.

When you click **Yes** in the confirmation message box, the primary node saves its configuration in a file and sends this to the secondary node. This file contains those configurations, which this document refers to as synchronized configuration. See How the Advanced Threat Defense cluster works? on page 284 for information on synchronized configuration. The secondary uses this configuration file to overwrite the corresponding configuration in its database. So, make sure that you have taken a backup of the secondary's configuration before you proceed. When you remove the secondary from the cluster, it retains the primary node's configuration.

7 Following a similar procedure, add the other secondary nodes.

The details of all nodes in the cluster are displayed in a table. Similar to other tables in the Advanced Threat Defense web application user-interfaces, you can sort the columns as well as hide or display the required columns.

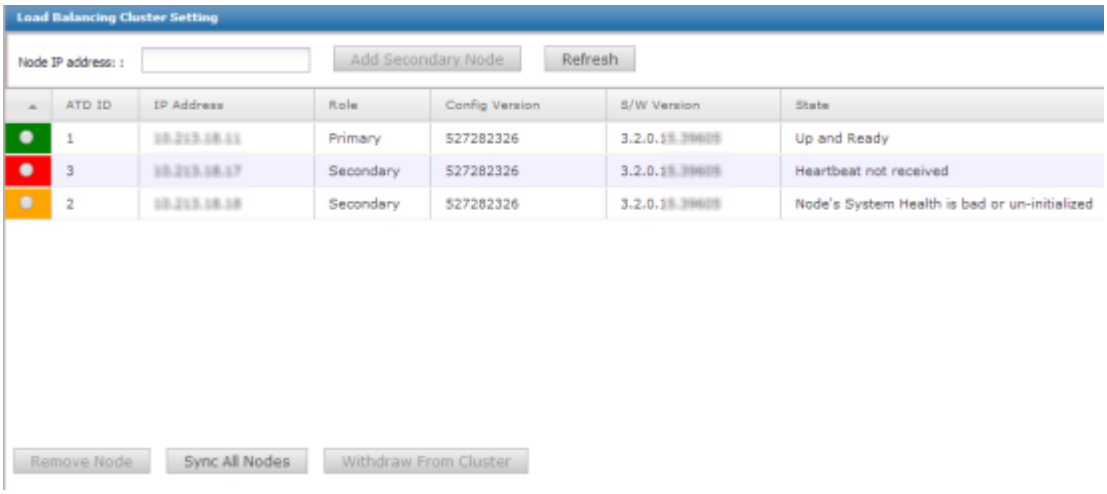



**Figure 8-5 Advanced Threat Defense cluster creation**

Except for **ATD ID**, **IP Address**, **Role**, and **Withdraw From Cluster**, none of the options are available in the **Load Balancing Cluster Setting** page for the secondary nodes.

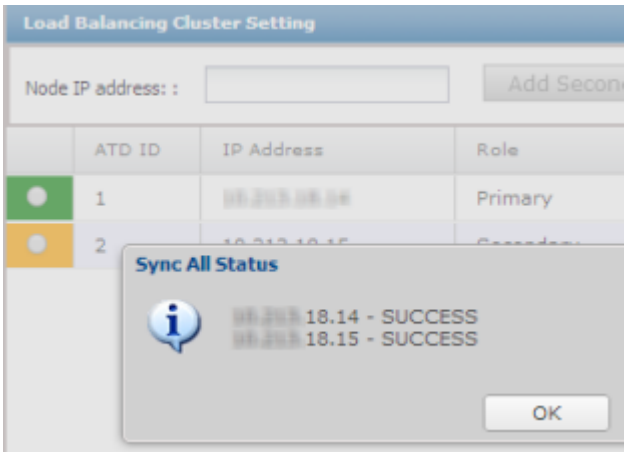
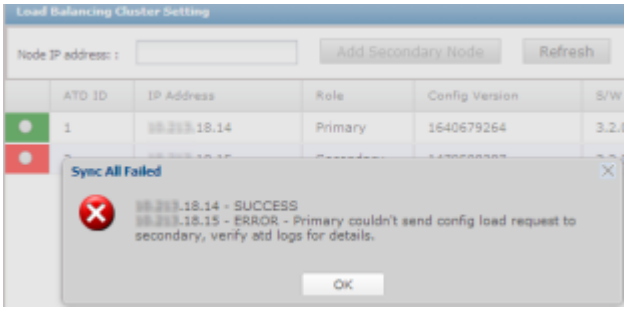
**Table 8-1 Option definitions**

| Option | Definition |
|---|---|
| **Node IP address** | Enter the management port IP address of the Advanced Threat Defense Appliance that you want to add to the cluster. |
| **Add Primary Node**<br>**Add Secondary Node** | Click to add the primary or the secondary node to the cluster.<br>The primary node or secondary node IP address is the IP address that you use to access the Advanced Threat Defense web application. |
| **Refresh** | Click to refresh the data displayed in the **Load Balancing Cluster Setting** page. The page is auto-refreshed every 15 seconds. |

**Table 8-1 Option definitions** *(continued)*

| Option | Definition |
|---|---|
| | Indicates the status of a node.<br>• : Indicates that the node is up and ready. If it is a secondary, it also means that the primary node is receiving the secondary's heartbeat signal.<br>• : Indicates that the node is up but needs your attention. For example, the configuration might not be in sync with that of the primary.<br>• : Indicates that the primary node is receiving the secondary node's heartbeat signal.<br>The primary node distributes files only to those nodes, which are in the green status. If the status of a secondary turns amber or red midway of a file transfer, the primary node allocates the file to the next node in queue. |
| **ATD ID** | This is a system-generated integer value to identify the nodes in a cluster. The primary node generates this unique value and assigns it to the nodes in the cluster.<br>This ID is displayed in the Analysis Status and Analysis Results left-hand-side tree structure on the primary node. This enables you to identify the node that analyzed a specific sample.<br>The uniqueness of the ATD ID is based on the IP address of a node as stored in the primary node's database. Consider that you have 3 nodes in the cluster. You remove the secondary node with ATD ID 2 from the cluster and add it back again to the cluster. Then this secondary node is assigned the same ATD ID of 2 if all these conditions are met:<br>• You have not changed the IP address of the node's eth-0 interface (management port).<br>• The primary node's database still has a record for the secondary's IP address. |
| **IP Address** | The management port IP address of the node. |
| **Role** | Indicates if a node is the primary or a secondary. |
| **Config Version** | When you save any of the synchronized configuration, the primary node sends its configuration file to the secondary nodes and also versions this configuration file for reference. For each node, the version number of its latest configuration file is displayed.<br>If the version number of a secondary node does not match with that of the primary, it indicates a possible difference in how the secondary node is configured. So, the status color for that secondary node turns to amber. The reason is also mentioned in the **State** column. Also, the primary node automatically pushes its configuration file to that node.<br>This ensures that all nodes are configured similarly concerning synchronized configuration. |
| **S/W Version** | Indicates the Advanced Threat Defense software version of the nodes. The complete software version must exactly match for all nodes. If not, the status turns to amber for the corresponding nodes. |
| **State** | Indicates the status of node and any critical information related to that node.<br>Some possible states are:<br>• Up and Ready<br>• Heartbeat not received.<br>• Node is on different config version. |

**Table 8-1 Option definitions** *(continued)*

| Option | Definition |
|---|---|
| **Remove Node** | Select a node and click to remove the node from the cluster. The configuration from the primary node is retained even when you remove a secondary node from the cluster. You cannot remove a primary node before you remove all secondary nodes.<br>This option is not available for a secondary node. |
| **Sync All Nodes** | Click **Sync All** to trigger the configuration-synchronization for all secondary nodes in the cluster.<br>When you add a secondary node or when you save any of the synchronized configuration in the primary node, the primary automatically triggers a synchronization to all secondary nodes in green and amber state.<br>Details of the configuration sync are displayed for each node based on the success or failure of the synchronization.<br>  <br>**Figure 8-6 Configuration sync success**<br>  <br>**Figure 8-7 Configuration sync error** |
| **Withdraw from Cluster** | This button is relevant only for secondary nodes. Click to withdraw a secondary node from the cluster and to use the secondary node as a standalone Advanced Threat Defense Appliance.<br>Recall that if the primary is down, the load-balancing cluster is down. If the primary is down, click **Withdraw from Cluster** in the secondary nodes to withdraw from the cluster and to use the secondary nodes as stand-alone appliances. |

# Monitor the status of an Advanced Threat Defense cluster

**Before you begin**

You have successfully created a load-balancing cluster as explained in Create the McAfee Advanced Threat Defense cluster on page 290.

You can monitor the status of an Advanced Threat Defense cluster in the **Load Balancing Cluster Setting** page or by using the `lbstats` command.

### Task

1 Log on to the CLI of the primary or a secondary node.

2 Run `lbstats` command.

Separate sections are displayed for each node.

```
ATD-3000> lbstats
<=== MY NODE INFO ===>
System Mode              : PRIMARY
ATD Id                   : 1
IP                       : 10.2
ATD Version              : 3.2.0.
Config Version           : 434480244
System Status            : ACTIVE(Up and Ready)
System Health            : GOOD


<=== SECONDARY NODE INFO ===>
System Mode              : SECONDARY
ATD Id                   : 2
IP                       : 10.2
ATD Version              : 3.2.0.
Config Version           : 434480244
System Status            : ACTIVE(Up and Ready)
System Health            : GOOD
Sample Files Distributed Count   : 33
ATD-3000>
```

**Figure 8-8 lbstats output from the primary node**

```
ATD-3000> lbstats
<=== MY NODE INFO ===>
System Mode              : SECONDARY
ATD Id                   : 2
IP                       : 10.
ATD Version              : 3.2.0.29.
Config Version           : 434480244
System Status            : ACTIVE(Up and Ready)
System Health            : GOOD

<=== PRIMARY NODE INFO ===>
System Mode              : PRIMARY
ATD Id                   : 1
IP                       : 10.
ATD-3000>
```

**Figure 8-9 lbstats output from a secondary node**

**Table 8-2 Details of the lbstats command**

| Output entry | Description |
|---|---|
| **System Mode** | Indicates whether the Advanced Threat Defense Appliance is the primary or a secondary node. |
| **ATD ID** | The unique ID assigned to the node. |

**Table 8-2 Details of the lbstats command** *(continued)*

| Output entry | Description |
|---|---|
| **IP** | The management port IP address of the Advanced Threat Defense Appliance. |
| **ATD Version** | Advanced Threat Defense software version currently installed on the node. |
| **Config Version** | The version of the configuration file currently on the node. |
| **System Status** | Whether the node is up and running. |
| **System Health** | Whether the node is in good or an uninitialized state. |
| **Sample Files Distributed Count** | The total number of samples distributed among the nodes, including the primary node. This node includes both files and URLs. This data is displayed only when you run `lbstats` on the primary node. |

## Submitting samples to an Advanced Threat Defense cluster

You use the primary node to submit samples to an Advanced Threat Defense cluster. The process is similar to how you use an individual Advanced Threat Defense Appliance.

- Make sure the integrated products interface with the primary node. When you configure the integration, make sure you use the passwords as configured in the primary node. For example, for Web Gateway, use the *mwg* user name and its password as configured in the primary node.
- To submit files and URLs manually, log on to the primary node with admin rights and submit the files just like how you submit the files to a standalone Advanced Threat Defense Appliance. See Upload files for analysis using McAfee Advanced Threat Defense web application on page 248 for step-by-step information.
- You can also use the REST APIs of the primary node to submit files and URLs. See the McAfee Advanced Threat Defense APIs Reference Guide for information.
- You can also submit files using FTP or SFTP to the primary node. See Upload files for analysis using SFTP on page 254.

## Monitor analysis status for an Advanced Threat Defense cluster

The **Analysis Status** page of the primary node displays the analysis status for files analyzed by each node. In a secondary node, only those files analyzed by that secondary node are displayed.

Similar to a standalone Advanced Threat Defense, you can view the status of samples that you submitted. If you have admin rights, you can view the status for samples submitted by any user.

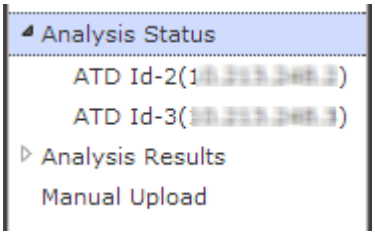
If a node is down after the primary node allotted a file to it, resubmit the file to the primary node.

### Task

1 Log on to the web application of the primary node.

2 Select **Analysis** | **Analysis Status**.

The **Analysis Status** expands to display the secondary nodes of the cluster. **Analysis Status** corresponds to the primary node. The secondary nodes are listed under **Analysis status** with their ATD ID and their management port IP address.




3 To view the status of the files analyzed by the primary node, click **Analysis Status**.

4 To view the status of files analyzed by a specific secondary node, click the corresponding ATD ID.

For the details of the options in the **Analysis Status** page, see Monitor the status of malware analysis on page 257.

## Monitor analysis results for an Advanced Threat Defense cluster

The **Analysis Results** page of the primary node displays the analysis results for files analyzed by each node. In a secondary node, only those files analyzed by that secondary node are displayed.

Similar to a standalone Advanced Threat Defense, you can view the results of samples that you submitted. If you have admin rights, you can view the results for samples submitted by any user.

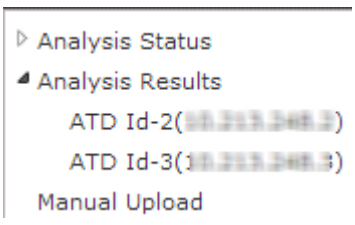
If a node is down after the primary node allotted a file to it, resubmit the file to the primary node.

### Task

1 Log on as the *admin* user in one of the nodes of the Advanced Threat Defense cluster.

2 Select **Analysis** | **Analysis Results**.

The **Analysis Results** expands to display the secondary nodes of the cluster. **Analysis Results** corresponds to the primary node. The secondary nodes are listed under **Analysis Results** with their ATD ID and their management port IP address.




3 To view the results of the files analyzed by the primary node, click **Analysis Results**.

4 To view the results of files analyzed by a specific secondary node, click the corresponding ATD ID.

For the details of the options in the **Analysis Results** page, see View the analysis results on page 259.

# Modifying configurations for a McAfee Advanced Threat Defense cluster

Regarding an McAfee Advanced Threat Defense cluster, configurations can be classified into two types:

- Settings that you configure only from the primary node. For the sake of explanation, these settings are referred as *synchronized configuration* in this document.
- Settings that you configure individually in each node of a McAfee Advanced Threat Defense cluster. These settings are referred as *unsynchronized configuration*.

**Synchronized configuration —** The following are the settings that fall under this category:

- Managing analyzer profiles on page 229
- Managing McAfee Advanced Threat Defense users on page 35
- Integration with McAfee ePO on page 234
- Specify proxy server for internet connectivity on page 235
- Configure the proxy DNS settings on page 236
- Configure date and time settings on page 237

Log on to the primary node with admin rights to configure these settings listed above. When you click **Save** in the corresponding pages, the primary node bundles the entire *synchronized configuration* in a file and sends it to all available secondary nodes. The secondary nodes save these settings in their database and use these settings later. This configuration file is assigned a version number. This version number is the **Config Version** listed in the **Load Balancing Cluster Setting** page.

The primary node sends the configuration file over a secure communication channel to the secondary nodes. You can verify the **State** column in the **Load Balancing Cluster Setting** page to verify if the configuration file was successfully applied on a secondary node. Alternatively, you can click **Sync All Nodes** in the **Load Balancing Cluster Setting** page for the primary node to send the configuration file to all available nodes. If a secondary node is down, it is indicated in the **State** column.

When the primary node synchronizes configuration for the cluster, it sends the complete *synchronized data* to all available nodes in the cluster. That is, you cannot selectively synchronize secondary nodes. Neither can you select the configurations that you want sent to the secondary nodes. However, the configuration-synchronization process does not affect the load-balancing or file-analysis processes of a McAfee Advanced Threat Defense Appliance.

**Unsynchronized configuration —** The following are the settings that fall under this category:

- Upgrade McAfee Advanced Threat Defense software from 3.0.2.xx to 3.0.4.xx on page 41.
- Creating analyzer VM on page 4
- Managing VM profiles on page 212
- DAT and engine versions of McAfee Anti-Malware Engine.
- DAT and engine versions of McAfee Gateway Anti-Malware Engine.
- Whitelist and blacklist entries.
- Custom YARA rules
- Database backup and restore configurations.
- Any configuration done using the CLI.

Log on to each node in the cluster to change these configurations. Make sure that these configurations are same in all nodes of the cluster.

# 9 CLI commands for McAfee Advanced Threat Defense

The McAfee Advanced Threat Defense Appliance supports command-line interface (CLI) commands for tasks such as network configuration, restarting the Appliance, and resetting the Appliance to factory defaults.

**Contents**


- *Issue of CLI commands*
- *CLI syntax*
- *Log on to the CLI*
- *Meaning of "?"*
- *Managing the disks of McAfee Advanced Threat Defense Appliance*
- *List of CLI commands*


## Issue of CLI commands

You can issue CLI commands locally, from the McAfee Advanced Threat Defense Appliance console, or remotely through SSH.

### How to issue a command through the console

For information on how to set up the console for a McAfee Advanced Threat Defense Appliance, see Configure network information for McAfee Advanced Threat Defense Appliance on page 29.

When the documentation indicates that you must perform an operation "on the Appliance," it signifies that you must perform the operation from the command line of a console host connecting to the McAfee Advanced Threat Defense Appliance. For example, when you first configure the network details for a McAfee Advanced Threat Defense Appliance, you must do so from the console.

When you are successfully connected to the McAfee Advanced Threat Defense Appliance, you will see the login prompt.

### Issuing a command through SSH

You can administer a McAfee Advanced Threat Defense Appliance remotely from a command prompt over `ssh`.

Only 5 SSHD CLI sessions can be open concurrently on a McAfee Advanced Threat Defense Appliance.

## Logging on to the McAfee Advanced Threat Defense Appliance using an SSH client

### Task

1 Open an SSH client session.

2 Enter the IPv4 address of the McAfee Advanced Threat Defense Appliance and enter 2222 as the SSH port number.

3 At the logon prompt, enter the default user name `atdadmin` and password `atdadmin`.

The number of logon attempts to the McAfee Advanced Threat Defense Appliance from a client, on a single connection, is set to 3, after which the connection is closed.

The number of logon attempts to the McAfee Advanced Threat Defense Appliance can differ based on the ssh client that you are using. You can get three logon attempts with certain clients (for example, Putty release 0.54, Putty release 0.56) or you can get four logon attempts with other clients (for example, Putty release 0.58, Linux ssh clients).

## Auto-complete

The CLI provides an auto-complete feature. To auto-complete a command, press **Tab** after typing a few characters of a valid command and then press **Enter**. For example, typing `pas` and pressing **Tab** would result in the CLI auto-completing the entry with the command `passwd`.

If the partially entered text matches multiple options, the CLI displays all available matching commands.

# CLI syntax

You issue commands at the command prompt as shown.

```
<command> <value>
```

- Values that you must enter are enclosed in angle brackets (< >).
- Optional keywords or values are enclosed in square brackets ([ ]).
- Options are shown separated by a line (|).
- Variables are indicated by *italics*.

Do not type the < or [ ] symbols.

## Mandatory commands

There are certain commands that must be executed on the McAfee Advanced Threat Defense Appliance before it is fully operational. The remaining commands in this chapter are optional and will assume default values for their parameters unless they are executed with other specific parameter values.

These are the required commands:

- `set appliance name`
- `set appliance ip`

- `set appliance gateway` is also required if any of the following are true:
  - If the McAfee Advanced Threat Defense Appliance is on a different network than the McAfee products you plan to integrate
  - If you plan to access McAfee Advanced Threat Defense from a different network either using an SSH client or a browser for accessing the McAfee Advanced Threat Defense Web Application

# Log on to the CLI

Before you can enter CLI commands, you must first log on to the McAfee Advanced Threat Defense Appliance with a valid user name (default user name is `atdadmin`) and password (default is `atdadmin`). To log off, type `exit`.

McAfee strongly recommends you change this password using the `passwd` command within your first interaction with the McAfee Advanced Threat Defense Appliance.

# Meaning of "?"

`?` displays the possible command strings that you can enter.

**Syntax**

`?`

If you use `?` in conjunction with another command, it shows the next word you can type. If you execute the ? command in conjunction with the `set` command, for example, a list of all options available with the `set` command is displayed.

# Managing the disks of McAfee Advanced Threat Defense Appliance

The McAfee Advanced Threat Defense Appliance has two disks referred to as disk-A and disk-B. Disk-A is the active disk and disk-B is the backup disk. Even if disk-A is not booted, it is referred as the active disk. Similarly, even if disk-B is the booted disk, it is referred as the backup disk. By default, both these disks contain the pre-installed software version. Subsequently, you can upgrade the software on the active disk, that is disk-A, and use disk-B to back up a stable version that you can always revert to.

Use the `show` command to view the software version stored in the active and backup disks.

**Table 9-1 CLI commands for managing the disks**

| Command | Description |
|---|---|
| `copyto backup` | Copies the software version on the active disk to the backup disk. For example, if you find the current active software version to be stable, you can back it up to the backup disk.<br>This command works only if the Appliance had been booted from the active disk. |
| `copyto active` | Copies the software version from the backup disk to the active disk. However, you must restart the McAfee Advanced Threat Defense Appliance for it to load this new image from the active disk.<br>This command works only if the Appliance had been booted from the backup disk. |
| `reboot backup` | Reboots the Appliance with the software version on the backup disk. |
| `reboot active` | Reboots the Appliance with the software version on the active disk. |

# List of CLI commands

This section lists McAfee Advanced Threat Defense CLI commands in the alphabetical order.

## amas

Use this command to restart/start/stop the amas services.

**Syntax**: `amas <word>`

| Parameter | Description |
|---|---|
| <WORD> | The amas service you want to stop. |

**Example:** `amas amas`

## atdcounter

Dsiplays the engine specific counter e.g. files sent and processed by GTI, MAV, GAM, Amas and so on.

**Syntax**: `atdcounter`

This command has no parameters.

## backup reports

Use this command to create a backup of the McAfee Advanced Threat Defense reports on an external FTP/SFTP server configured for a user under the FTP results output setting interface ports.

**Syntax**

`backup reports`

This command has no parameters.

## backup reports date

This command creates a backup of the McAfee Advanced Threat Defense reports for a particular date range on an external FTP/SFTP server configured for a user under the FTP results output setting.

**Syntax**: `backup reports date <yyyy-mm-dd>`

| Parameter | Description |
|---|---|
| yyyy-mm-dd yyyy-mm-dd | The date range for which you want to create a backup for reports. |

**Example:** `2014-07-10 2014-07-12`

## Blacklist

Use the following commands to manage the blacklist of McAfee Advanced Threat Defense.

**Syntax**:

- To add an MD5 to the blacklist, use `blacklist add <md5> <score> <file_name> <malware_name> <Eng-ID> <OS-ID>`

  | Parameter | Description |
  |---|---|
  | <md5> | The MD5 hash value of a malware that you want to add to the blacklist. |
  | <score> | The malware severity score. A valid value is from 3 to 5. |
  | <file_name> | The file name for the MD5. |
  | <malware_name> | The malware name for the MD5. |
  | <Eng-ID> | The numerical ID for the corresponding engine. |
  | <OS-ID> | The numerical ID of the operating system that was used to dynamically analyze the malware. |

  **Example**: `blacklist add 254A40A56A6E28636E1465AF7C42B71F 3 ExampleFileName ExampleMalwareName 3 3`

- To delete an MD5 from the blacklist, use `blacklist delete <md5>`

  | Parameter | Description |
  |---|---|
  | <md5> | The MD5 hash value of a malware that you want to delete from the blacklist. |

  **Example**: `blacklist delete 254A40A56A6E28636E1465AF7C42B71F`

- To check if an MD5 is present in the blacklist, use `blacklist query <md5>`

  | Parameter | Description |
  |---|---|
  | <md5> | The MD5 hash value of a malware that you want to query if it is present in the blacklist. |

  **Example**: `blacklist query 254A40A56A6E28636E1465AF7C42B71F`

  If the MD5 is present, the details such as the engine ID, malware severity score, and so on, are displayed.

- To update the details for an entry in the blacklist, use `blacklist update <md5> <score> <file_name> <malware_name> <Eng-ID> <OS-ID>`

| Parameter | Description |
|---|---|
| <md5> | The MD5 hash value of a malware that you want to update. This value must exist in the blacklist for you to update the record. |
| <score> | The new malware severity score that you want to change to. A valid value is from 3 to 5. |
| <file_name> | The new file name for the MD5. |
| <malware_name> | The new malware name for the MD5. |
| <Eng-ID> | The new engine ID that you want to change to. |
| <OS-ID> | The new value for the operating system that was used to dynamically analyze the malware. |

**Example**: `blacklist update 254A40A56A6E28636E1465AF7C42B71F 4 ExampleFileName ExampleMalwareName 3 4`

## clearstats

Resets all the McAfee Advanced Threat Defense statistics to zero.

**Syntax**: `clearstats`

This command has no parameters.

## createDefaultVms

Use this command to create default analyzer VMs.

**Syntax**: `createDefaultVms`

This command has no parameters.

## db_repair

Repairs the ATD database in case the database gets corrupt.

**Syntax**: `db_repair`

This command has no parameters.

## deleteblacklist

Use this command to remove all the entries from McAfee Advanced Threat Defense blacklist.

**Syntax**: `deleteblacklist`

This command has no parameters.

## deletesamplereport

Deletes all the analysis reports for a file.

**Syntax**: `deletesamplereport <md5>`

| Parameter | Description |
|---|---|
| <md5> | The MD5 value of the file for which you want to delete all the reports in McAfee Advanced Threat Defense. |

**Example**: `deletesamplereport c0850299723819570b793f6e81ce0495`

## diskcleanup

Use this command to delete some of the older analysis reports if the disk space of McAfee Advanced Threat Defense is low.

**Syntax**: `diskcleanup`

This command has no parameters.

## Exit

Exits the CLI.

This command has no parameters.

**Syntax**:

`exit`

## factorydefaults

Deletes all samples, results, logs, and analyzer VM images, and it resets IP addresses before rebooting the device. This command does not appear when you type `?` nor does the auto-complete function applies to this command. You must type the command in full to execute it.

This command has no parameters.

- You are warned that the operation will clear McAfee Advanced Threat Defense Appliance and you must confirm the action. The warning occurs since the McAfee Advanced Threat Defense Appliance returns to its clean, pre-configured state, thus losing all current configuration settings in both the active and backup disks. Once you confirm, this command immediately clears all your configuration settings, including samples, results, logs, and analyzer VM images, in both the active and backup disks.
- The current software version in the backup disk is applied on the active disk.

**Syntax**:

`factorydefaults`

## ftptest USER_NAME

Use this command to test the FTP settings saved under MANAGE > USER MANAGEMENT > FTP Results (for a particular user).

**Syntax**: `ftptest USER_NAME`

| Parameter | Description |
|---|---|
| USER_NAME | The user name for which you want to test the FTP settings |

**Example:** `NSPuser`

## gti-restart

Restarts the McAfee GTI engine of McAfee Advanced Threat Defense.

**Syntax**: `gti-restart`

This command has no parameters.

## help

Provides a description of the interactive help system.

This command has no parameters.

**Syntax**:

```
help
```

## heuristic_analysis

Consider a scenario where there is a very high volume of files submitted by a Network Security Sensor. You want McAfee Advanced Threat Defense to triage these files based on a need for detailed malware analysis. The intention of this triage is to scale up performance without compromising on security. The heuristic_analysis command is introduced to meet such a requirement.

- Enable the heuristic filter for PDF files.
- Specify the minimum file size for PDF files to qualify for malware analysis.
- Disable the re-analyze option for all supported file types.

Use the `show` command to know the current status. By default, heuristic analysis is disabled.

**Syntax**: `show heuristic_analysis`

When heuristic analysis is disabled, the following are the settings:

| Setting | Description |
|---|---|
| `Heuristic filtering is OFF` | This is a feature of McAfee Advanced Threat Defense. When turned on, McAfee Advanced Threat Defense does a heuristic analysis of a PDF file submitted by Network Security Sensor. That is, it examines the structure of the PDF file for any malicious content such as embedded Java scripts, embedded .exe files, or any redirections. Only if there are heuristic abnormalities in the file, it is considered for malware analysis as per the corresponding analyzer profile. If there are no abnormalities, the file is treated as clean. That is, a severity rating of zero (information) is assigned.<br>In networks where there is a very high flow of PDF files, the heuristic filter can reduce the load on McAfee Advanced Threat Defense by filtering off files that do not have any suspicious content. |
| `configuration setting: re-analysis: ON` | By default, McAfee Advanced Threat Defense analysis all the supported files submitted by a Sensor even if the files have already been analyzed. When re-analysis is set to OFF, McAfee Advanced Threat Defense checks if analysis results are already available for a file based on its MD5 hash value. If yes, then it provides the available result to Network Security Manager instead of re-analyzing the file. |
| `configuration setting: min file size: 2048` | For PDF files submitted by Sensors, you can specify a minimum file size. Files that are lesser than this size are not analyzed by McAfee Advanced Threat Defense. This reduces the load on McAfee Advanced Threat Defense by filtering off small PDF files. The default file size for PDF files submitted by Sensors is 2 KB. You cannot specify a value less than 2 KB (2048 bytes). |

The re-analysis function applies to all supported file types supported by Sensors, whereas the heuristic filter and minimum file size apply only to PDF files submitted by Sensors.

Use the `set` command to enable or disable heuristic analysis for files submitted by a Sensor.

**Syntax**: `set heuristic_analysis <enable> <PDF minimum file size in bytes>`

**Syntax**: `set heuristic_analysis <disable>`

The `set heuristic_analysis` command does not execute when analyzer VM creation is in progress.

**Example without minimum file size**: `set heuristic_analysis enable`

If you execute this example, the following settings are applied in the same order for PDF files submitted by a Sensor:

1. Since you have not specified a minimum file size, it is set to 2 KB. So, McAfee Advanced Threat Defense considers only PDF files of size 2 KB or more for further analysis.
2. Enabling heuristic analysis sets re-analysis to OFF. So, McAfee Advanced Threat Defense checks if the analysis result is already available. If yes, this result is forwarded to the Manager without further analysis. If the result is not available for the same MD5 hash value, the analysis proceeds to the next step.
3. Enabling heuristic analysis sets heuristic filter to ON. So, McAfee Advanced Threat Defense checks the PDF file structure for any abnormalities. If there are no abnormalities, the file is treated as clean and there is no further analysis. If there are any heuristic abnormalities, the PDF file is statically and dynamically analyzed as per the corresponding analyzer profile.

For non-PDF files, only the re-analysis option (step 2 above) is considered.

**Example with minimum file size**: `set heuristic_analysis enable 5000`

If you execute this example, the following settings are applied in the same order for PDF files submitted by a Sensor:

1 The minimum file size is set to 5000 bytes. So, McAfee Advanced Threat Defense considers only PDF files of size 5000 bytes or more for further analysis.

2 Enabling heuristic analysis sets re-analysis to OFF. So, McAfee Advanced Threat Defense checks if the analysis result is already available. If yes, this result is forwarded to the Manager without further analysis. If the result is not available for the same MD5 hash value, the analysis proceeds to the next step.

3 Enabling heuristic analysis sets heuristic filter to ON. So, McAfee Advanced Threat Defense checks the PDF file structure for any abnormalities. If there are no abnormalities, the file is treated as clean and there is no further analysis. If there are any heuristic abnormalities, the PDF file is statically and dynamically analyzed as per the corresponding analyzer profile.

For non-PDF files, only the re-analysis option (step 2 above) is considered.

**Example for disabling heuristic analysis**: `set heuristic_analysis disable`

If you execute this example, the following settings are applied:

1 The minimum file size is set to the default value of 2048 bytes.

2 Disabling heuristic analysis sets re-analysis to ON. So, McAfee Advanced Threat Defense analyzes all supported files submitted by Sensors regardless of whether results are already available or not for that file.

3 Disabling heuristic analysis sets heuristic filter to OFF. So, McAfee Advanced Threat Defense does not check PDF files for any heuristic abnormalities. The PDF files are statically and dynamically analyzed as per the corresponding analyzer profile.

## lbstats

Shows the statistics for nodes in a load-balancing cluster.

This command has no parameters. No output is displayed if the Advanced Threat Defense is not part of a cluster.

**Syntax**:

```
lbstats
```

For the details see, Monitor the status of an Advanced Threat Defense cluster on page 293.

## list

Lists all the CLI commands available to users.

**Syntax**: `list`

This command has no parameters.

## lowseveritystatus

Advanced Threat Defense treats severity 1 and 2 samples as low-severity and severity 3, 4, and 5 as malicious. By default, if you configure dynamic analysis, the dynamic analysis score is displayed in the summary report for all samples. This score also affects the final score for that sample. If necessary,

you can use the `lowseveritystatus` command to alter this behavior. For example, for low-severity samples that are dynamically analyzed, Advanced Threat Defense does not display the dynamic analysis score in the summary report nor consider this score for computing the final score.

The `lowseveritystatus` command applies only to non-PE samples such as Microsoft Word documents and PDF files.

**Syntax**: `lowseveritystatus <show><hide>`

**Example**: `lowseveritystatus hide`

| Parameter | Description |
|---|---|
| `show` | This is the default behavior. If a sample is dynamically analyzed, Advanced Threat Defense displays the dynamic analysis score in the report. It also considers this score to compute the final score. |
| `hide` | Assume that the sample is a non-PE file, which has undergone dynamic analysis. If Advanced Threat Defense detects the file to be low-severity, it does not display the dynamic analysis score in the report (under **Sandbox** in the **Down Selector's Analysis** section). Advanced Threat Defense also does not consider the dynamic analysis score for computing the final score. However, the details of the dynamic analysis such as files opened and files created are included in the report.<br>The `lowseveritystatus hide` command affects only the score displayed in the report and does not affect how the results are displayed in the **Analysis Results** page. |

## nslookup

Displays nslookup query result for a given domain name. You can use this to verify if McAfee Advanced Threat Defense is able to perform nslookup queries correctly.

**Syntax**: `nslookup <WORD>`

| Parameter | Description |
|---|---|
| <WORD> | The domain name for which you want to query for nslookup. |

**Example:** `nslookup mcafee.com`

## passwd

Changes the password of the CLI user (atdadmin). A password must be between 8 and 25 characters in length and can consist of any alphanumeric character or symbol.

You are asked to enter the current password before changing to a new password.

**Syntax**:

```
passwd
```

## ping

Pings a network host. You can specify an IPv4 address.

**Syntax**:

```
ping <A.B.C.D>
```

| Parameter | Description |
|---|---|
| <A.B.C.D> | denotes the 32-bit IP address written as four eight-bit numbers separated by periods. Each number (A, B, C or D) is an eight-bit number between 0–255. |

## quit

Exits the CLI.

This command has no parameters.

**Syntax**:

```
quit
```

## reboot

Reboots the McAfee Advanced Threat Defense Appliance with the image in the current disk. You must confirm that you want to reboot.

**Syntax**:

```
reboot
```

| Parameter | Description |
|---|---|
| `reboot active` | Reboots the Appliance with the software version on the active disk. |
| `reboot backup` | Reboots the Appliance with the software version on the backup disk. |
| `reboot vmcreator` | Recreates the analyzer VMs configured in the McAfee Advanced Threat Defense web application, while rebooting the Appliance. |

## resetuiadminpasswd

Use this command to reset the password for the *admin* user of McAfee Advanced Threat Defense web application. When you execute this command, the password is reset to the default value, which is *admin*. Note that the currently logged on sessions are not affected. A change in password affects only new logon attempts.

**Syntax**: `resetuiadminpasswd`

Press Y to confirm or N to cancel.

## resetusertimeout

Enables users to log on to McAfee Advanced Threat Defense web application without waiting for the timer to expire.

**Syntax**: `resetusertimeout <WORD>`

| Parameter | Description |
|---|---|
| <WORD> | The McAfee Advanced Threat Defense web application user name for which you want to remove the logon timer. If this action is successful, the message *Reset done!* is displayed. |

**Example:** `resetusertimeout admin`

## route add/delete network

CLI commands are available for adding and deleting static route to McAfee Advanced Threat Defense.

**To add a port**

```
route add network <network ip> netmask <netmask> gateway <gateway ip> intfport <port number 1><port number 2><port number 3>
```

Example: `route add network 1.1.1.0 netmask 255.255.255.0 gateway 1.1.1.1 intfport 1`

**To delete a port**

```
route delete network <network ip> netmask <netmask> gateway <gateway ip> intfport <port number 1><port number 2><port number 3>
```

Example: `route delete network 1.1.1.0 netmask 255.255.255.0 gateway 1.1.1.1 intfport 1`

## samplefilter

This command is specific to Network Security Platform Sensors. Use this command to prevent Sensors from sending unsupported file types to McAfee Advanced Threat Defense for analysis.

**Syntax**:

```
samplefilter <status><enable><disable>
```

| Parameter | Description |
|---|---|
| status | displays whether the sample filtering feature is enabled or disabled currently. By default, it is enabled. |
| enable | sets the sample filtering on. When it is enabled, McAfee Advanced Threat Defense considers only the supported file types from Network Security Platform for analysis. Refer to Analyzing malware on page 4 for the list of supported files.<br>McAfee Advanced Threat Defense ignores all other file types and also informs Network Security Platform that a sample is of an unsupported file type . This prevents resources being spent on unsupported file types on both McAfee Advanced Threat Defense and Network Security Platform. |
| disable | sets the sample filtering to off. When disabled, McAfee Advanced Threat Defense considers all the files submitted by Network Security Platform for analysis but only the supported file types are analyzed. The remaining are reported as unsupported in the **Analysis Status** and **Analysis Results** pages. |

**Example**:

```
samplefilter status
```

## set appliance ip

Specifies the McAfee Advanced Threat Defense Appliance IPv4 address and subnet mask. Changing the IP address requires a restart for the changes to take effect. See the `reboot` command for instructions on how to reboot the McAfee Advanced Threat Defense Appliance.

**Syntax**:

```
set appliance ip <A.B.C.D E.F.G.H>
```

| Parameter | Description |
|---|---|
| <A.B.C.D E.F.G.H> | indicates an IPv4 address followed by a netmask. The netmask strips the host ID from the IP address, leaving only the network ID. Each netmask consists of binary ones (decimal 255) to mask the network ID and binary zeroes (decimal 0) to retain the host ID of the IP address(For example, the default netmask setting for a Class C address is 255.255.255.0). |

**Example**:

```
set appliance ip 192.34.2.8 255.255.0.0
```

## set appliance gateway

Specifies IPv4 address of the gateway for the McAfee Advanced Threat Defense Appliance.

**Syntax:**

```
set appliance gateway <A.B.C.D>
```

| Parameter | Description |
|---|---|
| <A.B.C.D> | a 32-bit address written as four eight-bit numbers separated by periods. A, B, C or D represents an eight-bit number between 0–255. |

**Example:**

```
set appliance gateway 192.34.2.8
```

## set appliance name

Sets the name of the McAfee Advanced Threat Defense Appliance. This name is used to identify the McAfee Advanced Threat Defense Appliance if you integrate it with Network Security Platform.

**Syntax**:

```
set appliance name <WORD>
```

| Parameter | Description |
|---|---|
| <WORD> | indicates a case-sensitive character string up to 25 characters. The string can include hyphens, underscores, and periods, and must begin with a letter. |

**Example**:

```
set appliance name SanJose_MATD1
```

## set intfport

Use this command to enable or disable McAfee Advanced Threat Defense interface ports.

**Syntax**

```
set intfport <1><2><3> <enable><disable>
```

Example: `set intfport 1 enable`

## set intfport auto

Sets an interface port to auto-negotiate the connection with the immediate network device.

**Syntax:**

```
set intfport <1><2><3> auto
```

**Example:**

```
set intfport 1 auto
```

## set intfport ip

Sets an IP address to an interface port.

**Syntax:**

```
set intfport <1><2><3> ip A.B.C.D E.F.G.H
```

**Example:**

```
set intfport 1 10.10.10.10 255.255.255.0
```

## set intfport speed duplex

Set the speed and duplex setting on the specified interface port.

**Syntax:**

```
set intfport <1><2><3> speed <10 | 100> duplex <half | full>
```

| Parameter | Description |
|---|---|
| <1> <2> <3> | Enter an interface port ID for which you want to set the speed and duplex. |
| <10 \| 100> | Sets the speed on the interface port. The speed value can be either 10 or 100 |
| <half \| full> | Sets the duplex setting on the interface port. Set the value "half' for half duplex and full for 'full' duplex. |

**Example:**

```
set intfport 1 speed 100 duplex full
```

## set malware-intfport

Configure the required port to route Internet traffic from an analyzer VM.

Before you run this command, make sure that the required port is enabled and configured with an IP address.

**Syntax:** `set malware-intfport <1><2><3> gateway A.B.C.D`

**Example:** `set malware-intfport 1 10.10.10.252`

Run the `show intfport 1` and verify the `Malware Interface Port` and `Malware Gateway` entries.

McAfee Advanced Threat Defense uses the configured port to provide Internet access to analyzer VMs. See Internet access to sample files on page 226.

## set mgmtport auto

Configures the network port to auto-negotiate the connection between the McAfee Advanced Threat Defense Appliance and the immediate network device.

This command has no parameters.

**Syntax**:

```
set mgmtport auto
```

**Default Value**:

By default, the network port is set to **auto** (auto-negotiate).

## set mgmtport speed and duplex

Configures the network port to match the speed of the network device connecting to the McAfee Advanced Threat Defense Appliance and to run in full- or half-duplex mode.

**Syntax:**

```
set mgmtport <speed <10 | 100> duplex <full | half>>
```

| Parameter | Description |
|---|---|
| <10\|100> | sets the speed on the Ethernet network port. The speed value can be either 10 or 100 Mbps. To set the speed to 1000 Mbps, use the `set mgmtport auto` command. |
| <half\|full> | sets the duplex setting on the Ethernet network port. Set the value `half` for half duplex and `full` for full duplex. |

**Default Value:**

By default, the network port is set to **auto** (auto-negotiate).

## set fips

Enable or disable FIPS mode. This command has no parameters. Restart the McAfee Advanced Threat Defense Appliance when you enable or disable FIPS mode.

**Syntax**: `set fips <enable> <disable>`

## set ftp

When you upload files for analysis using an FTP client or when you import a VMDK file into McAfee Advanced Threat Defense to create an analyzer VM, you use SFTP since FTP is not supported by default. However, if you prefer to use FTP for these tasks, you can enable FTP.

**Syntax**: `set ftp <enable><disable>`

By default, FTP is disabled.

**Example**: `set ftp enable`

See also: show ftp on page 316.

## set heuristic_analysis

See heuristic_analysis on page 306.

## set ui-timeout

Specifies the number of minutes of inactivity that can pass before the McAfee Advanced Threat Defense web application connection times out.

**Syntax**:

```
set ui-timeout <60 - 86400>
```

| Parameter | Description |
|---|---|
| <60 - 86400> | You can set a timeout period from 60 to 86400 seconds. |

**Example**: `set ui-timeout 600`

**Default Value**: 15 minutes

## set whitelist

Use this command to configure checking of whitelist by McAfee Advanced Threat Defense. By default, it is enabled.

**Syntax**: `set whitelist <enable><disable>`

**Example**: `set whitelist enable`

## show

Shows all the current configuration settings on the McAfee Advanced Threat Defense Appliance.

This command has no parameters.

**Syntax**:

`show`

Information displayed by the `show` command includes:

[Sensor Info]

- System Name
- Date
- System Uptime
- System Type
- Serial Number
- Software Version
- Active Version
- Backup Version
- MGMT Ethernet Port

[Sensor Network Config]

- IP Address
- Netmask
- Default Gateway

## show epo-stats nsp

Displays the count of requests sent to McAfee ePO, the count of responses received from McAfee ePO, and the count of requests that failed.

**Syntax:** `show epo-stats nsp`

This command has no parameters.

## show fips

Shows if FIPS is enabled or disabled currently. This command has no parameters.

**Syntax**: `show fips`

## show ftp

Use this command to know if FTP is enabled or disabled currently. By default, FTP is disabled.

**Syntax**: `show ftp`

See also: set ftp on page 314.

## show history

Displays the list of CLI commands issued in this session.

**Syntax:** `show history`

This command has no parameters.

## show heuristic_analysis

See heuristic_analysis on page 306.

## show intfport

Shows the status of the specified interface port or the management port of McAfee Advanced Threat Defense.

**Syntax**: `show intfport <mgmt><1><2><3>`

Information displayed by the `show intfport` command includes:

- Whether the port's administrative status is enabled or disabled.
- The port's link status.
- The speed of the port.
- Whether the port is set to half or full duplex.
- Total packets received.
- Total packets sent.
- Total CRC errors received.
- Total other errors received.
- Total CRC errors sent.
- Total other errors sent.
- IP address of the port.
- MAC address of the port.
- Whether the port is used to provide Internet access to analyzer VMs.
- If configured to provide Internet access to analzyer VMs, then the corresponding gateway for this traffic.

## show nsp scandetails

Shows the file scan details regarding the integrated IPS Sensors.

**Syntax**: `show nsp scandetails <Sensor IP address>`

If you do not specify the Sensor IP address, the details are displayed for all the Sensors integrated with the McAfee Advanced Threat Defense Appliance.

Information displayed by the `show nsp scandetails` command includes:

- The IP address of the IPS Sensor.
- Total number of packets received from the Sensor.
- Total number of packets sent to the Sensor.
- The timestamp of when the last packet was sent to and received from the Sensor.
- The encryption method used for the communication with the Sensor.
- Session handle null counts.
- Count of internal errors.
- Count of unknown commands received from the Sensor.
- File string null.
- File data null.
- Count of unknown files.
- Count of out of order packets.
- Count of MD5 mismatches between what was sent by the Sensor and what was calculated by McAfee Advanced Threat Defense.
- Count of memory allocation failures.
- File transfer timeout.
- New file count.
- Count of shared memory allocation failures.
- Count of the number of static analysis responses sent.
- Count of the number of dynamic analysis responses sent.
- Count of scan request received.
- MD5 of the last file that was streamed by the Sensor.

## show route

This command is used to show routes that you configured using the `route add` command as well as the system IP routing table.

**Syntax:**

```
show route
```

The details from a sample output of the command in the following table.

**Table 9-2 System IP routing table**

| Destination | Gateway | Genmask | Flags | Metric | Ref | Use | Iface |
|---|---|---|---|---|---|---|---|
| 10.10.10.0 | 0.0.0.0 | 255.255.255.0 | U | 0 | 0 | 0 | mgmt |
| 11.11.11.0 | 0.0.0.0 | 255.255.255.0 | U | 0 | 0 | 0 | mgmt |
| 12.12.0.0 | 0.0.0.0 | 255.255.0.0 | U | 0 | 0 | 0 | mgmt |
| 13.0.0.0 | 0.0.0.0 | 255.0.0.0 | U | 0 | 0 | 0 | mgmt |
| 0.0.0.0 | 10.10.10.253 | 0.0.0.0 | UG | 0 | 0 | 0 | mgmt |

## show ui-timeout

Displays the McAfee Advanced Threat Defense web application client timeout in seconds.

**Syntax:** `show ui-timeout`

**Sample output:** `Current timeout value: 1200`

## shutdown

Halts the McAfee Advanced Threat Defense Appliance so you can power it down. Then, after about a minute, you can power down the McAfee Advanced Threat Defense Appliance **manually** and unplug both the power supplies. McAfee Advanced Threat Defense Appliance does not power off automatically. You must confirm that you want to shut it down.

This command has no parameters.

**Syntax**:

```
shutdown
```

## status

Shows McAfee Advanced Threat Defense system status, such as the health and the number of files submitted to various engines.

This command has no parameters.

**Syntax**: `status`

**Sample output**:

```
System Health Status : good

Sample files received count: 300

Sample files submitted count: 300

GTI Scanner files submitted count: 50

GAM Scanner files submitted count: 100

MAV Scanner files submitted count: 200

Sandbox files submitted count: 25

Sandbox files finished count: 25

Sample files finished count: 300

Sample files error count: 0
```

## update_avdat

By default, McAfee Advanced Threat Defense updates the DAT files for McAfee Gateway Anti-Malware Engine and McAfee Anti-Malware Engine every 90 minutes. To update these files immediately, use the `update_avdat` command.

This command has no parameters.

**Syntax**: `update_avdat`

## Vmlist

Displays list of all the VMs configured on the McAfee Advanced Threat Defense

**Syntax**: `vmlist`

## watchdog

The watchdog process reboots the McAfee Advanced Threat Defense Appliance whenever an unrecoverable failure is detected.

**Syntax**:

`watchdog <on | off | status>`

| Parameter | Description |
|---|---|
| <on> | Enables the watchdog. |
| <off> | Disables the watchdog. Use it if the Appliance reboots continuously due to repeated system failure. |
| <status> | Displays the status of the watchdog process. |

## set malware-intfport mgmt

By default, Internet access to analyzer VMs is through the McAfee Advanced Threat Defense's management port (eth-0). Use this command, if you had configured a different port for routing Internet traffic and want to revert to the management port.

**Syntax:** `set malware-intfport mgmt`

Run the `show intfport mgmt` and verify the `Malware Interface Port` and `Malware Gateway` entries.

McAfee Advanced Threat Defense uses the management port to provide Internet access to analyzer VMs. See Internet access to sample files on page 226.

## whitelist

Use the following commands to manage the whitelist of McAfee Advanced Threat Defense.

**Syntax**:

- To add an MD5 to the whitelist, use `whitelist add <md5>`

  **Example**: `whitelist add 254A40A56A6E68636E1465AF7C42B71F`

- To delete an MD5 from the whitelist, use `whitelist delete <md5>`

  **Example**: `whitelist delete 254A40A56A6E28836E1465AF7C42B71F`

- To check if an MD5 is present in the whitelist, use `whitelist query <md5>`

  **Example**: `whitelist query 254A40A56A6E28636E1465AF7C42B71F`

- To check the status if checking the whitelist status is currently enabled, use `whiteliststatus`

# Index


## A

about this guide 7
active disk 301
analysis results
    cluster 297
    viewing 259
analysis status
    cluster 296
    monitoring 257
analyzer profile 221
    adding 231
    deletion 233
    management 229
    modification 233
    viewing 230
analyzer VM 221
    creating 61
Anti-Malware Engine 221

## B

backup and restore 54
backup disk 301

## C

CLI commands
    how to? 299
    list 302
    mandatory commands 300
    syntax 300
CLI commands issue
    auto-complete 300
    console 299
    ssh 299
CLI logon 301
conventions and icons used in this guide 7
custom YARA rules 240

## D

dashboard 274
database
    backup and restore 54
date and time 237, 242, 245, 246
diagnostic files 52
disk-A 301
disk-B 301
DNS settings configuration 236
documentation
    product-specific, finding 8
    typographical conventions and icons 7
dynamic analysis 221

## E

ePO server configuration 235
ePO server integration 234
exporting logs 52

## G

Gateway Anti-Malware Engine 221

## I

Internet access 226
Internet proxy server 235

## J

JSON 261

## L

local blacklist 221
local whitelist 221
log files 52

## M

malware analysis 247
    process flow 225, 247, 254
malware analysis configuration
    high-level steps 225
    overview 221
McAfee Advanced Threat Defense
    accessing web application 34
    advantages 14
    backup and restore 54
    dashboard 274
    deployment options 12
    disks 301
    performance monitoring 40

McAfee Advanced Threat Defense *(continued)*
performance monitors 278
software import 41, 47
solution description 10
upgrade 41, 47
user management 35
McAfee Advanced Threat Defense Appliance
hardware specifications 23
important information 18
setting up 17, 25
McAfee ServicePortal, accessing 8
monitors
malware analysis 275
VM creation status 278

## N

Network Simulator 226

## O

OpenIOC 261
overview 9

## P

port numbers used 25
process flow 234

## R

real Internet mode 226
reports
analysis summary 261
disassembly results 267
dropped files 267
logic path graph 268

## S

sample analysis 247
Sensor logon; ssh 300
ServicePortal, finding product documentation 8
simulation mode 226
static analysis 221
STIX 261
support bundle 52
system requirements
client 33

## T

technical support, finding product information 8
terminologies 221
troubleshooting 52

## U

upload files
manual 248
SFTP 254
web application 248
upload samples
manual 248
SFTP 254
web application 248
upload URLs
manual 255
user-interactive mode 249
web application 255
user 221
user API log 273
user interactive mode 249

## V

view analysis results 259
VM creation log 220
VM profile 221
adding 214
creating 214
deleting 220
editing 219
management 212
viewing 213
VMDK file
image conversion 209
importing 208

## W

Warnings 19

## X

X-Mode 249
XML 261
XMode 249

## Y

YARA rules 240

McAfee
An Intel Company